

#4

実光様王姓
 国名 アメリカ合衆国
 出願 1975年2月24日
 出願番号 第532084号
 特許 第1111号
 昭和51年2月17日

特許庁長官 片山石郎殿
 1.発明の名称
 暗号装置
 2.発明者
 住所 アメリカ合衆国ニューヨーク州マンハッタン
 氏名 アイリッシュ・エフ・エイムズ(他4名)
 3.特許出願人
 住所 アメリカ合衆国10504、ニューヨーク州
 名 氏 インターナショナル・ビジネス・マシーンズ・コーポレーション
 (709)
 代表者 ジェイ・エイ・グレイデー
 国 籍 アメリカ合衆国
 4.代理人
 住所 郵便番号 104
 東京都港区六本木三丁目2番12号
 日本アイ・ビー・エム株式会社
 Tel(代表)586-1111
 氏名 伊藤士小野 廣司
 (6454)
 5.交付審議の目的
 (1) 明 細 書 1通
 (2) 図 面 1通
 (3) 発明の概要 1通
 (4) 優先権主張書及訳文 各1通
 (5) 出願審査請求書 1通

① 日本国特許庁 公開特許公報

①特開昭 51-108701
 ④公開日 昭51.(1976)9.27
 ②特願昭 51-16096
 ⑤出願日 昭51.(1976)2.18
 審査請求 有 (全32頁)

庁内整理番号
 6964 53
 7240 53
 7165 56

②日本分類
 9601D0
 9607A1
 9707E2

⑤Int.Cl.³
 H04K 1/00
 H04L 9/00
 G06F 3/00

Best Available Copy

明 細 書

1.発明の名称 暗号装置。
 2.特許請求の範囲
 (1) 一組の暗号キー・ビットの制値のもとにデータ・ビットのブロックに対して換ブロック暗号処理操作を実行するための暗号装置にして、
 上記データ・ビットのブロックを記憶するための記憶手段と、
 上記一組の暗号キー・ビットを置換して出力するための第1線形変換手段と、
 上記記憶手段に蓄積され、上記データ・ビットのブロックを拡張することにより、上記第1線形変換手段から出力された暗号キー・ビットの数の新しいデータ・ビットのブロックを生成するための手段と、
 該手段からの拡張されたデータ・ビットのブロック及び上記第1線形変換手段からの置換された暗号キー・ビットに従って代替変換を実行することにより、元のデータ・ビットの数の等しいビット数を有する代替ビット群を生成するための手段と、
 該手段から出力された上記代替ビット群を復換することにより、上記データ・ビットのブロックの復ブロック暗号を生成するための第2線形変換手段とを有することを特徴とする暗号装置。

しいビット数を有する代替ビット群を生成するための手段と、
 該手段から出力された上記代替ビット群を復換することにより、上記データ・ビットのブロックの復ブロック暗号を生成するための第2線形変換手段とを有することを特徴とする暗号装置。
 (2) 上記代替ビット群を生成するための手段が、拡張されたデータ・ビット及び置換された暗号キー・ビットを組合わせて新しい一組のビットを生成するための手段と、
 該手段から出力された上記一組のビットに対して非線形代替変換を施すことにより上記代替ビット群を生成するための非線形変換手段とより成ることを特徴とする特許請求の範囲第1項記載の暗号装置。

3 発明の詳細な説明

本発明は、データ処理環境のもとで利用される暗号装置に関するものであり、更に具体的には、データの機密保護及びプライバシーを確立するため、デジタル・データを暗号化したり解読したりするのに使用される積ソロシ暗号プロセスを遂行するための暗号装置に関するものである。

コンピュータ・システム・ネットワークにおける遠隔通信の利用、端末即ち入出力装置と制御装置との間の非常に長いケーブル接続の使用、及び記憶媒体の移動可能性が各々増大するにつれて、データの物理的な保護が一般に保証されなくなつてきたために、データの紛失又は悪用に対する関心が高まつてきた。暗号方式は、データの伝送媒体よりもむしろデータ自身を保護するという点において、データの機密性及びプライバシーの保護を達成するための1つの手段として認められている。

これまでにも、データ通信の機密保護及びプライバシーの維持を目的として、メッセージを暗号

特開：昭51-108701(2)

化するための種々のシステムが開発されている。このようにシステムの一つは、ブロック全体が所定の暗号キーに従つて代替(substitute)されるようなブロック暗号システムがある。代替されたメッセージは、暗号キーを知らなければ解読されない暗号テキストになる。所定の暗号キーに従つて処理が行なわれる代替技術(substitution technique)の利点は、この暗号キーを適切に適用することによつて暗号操作を簡単に実行できることにある。代替技術の設計及び処理に関する更に詳しい説明は、例えば1949年10月に発行されたBell System Technical Journal, 第28巻、第656~715頁に掲載されているC. E. Shannonによる"Communication Theory of Secrecy Systems"と題する論文及び1973年5月に発行されたScientific American, 第228巻、第5号、第15~23頁に掲載されているH. Feistelによる"Cryptography and Computer Privacy"と題する論文に見出される。これら

2つの論文には、2以上の暗号が、例えば非線形代替及びこれに続く線形変換といった連続的な段階によつて、連続的に組合わされるような積暗号システムについての詳しい説明がなされている。

データ処理システム内でのデータの機密保護及びプライバシーを改善するため、種々の積暗号システムが開発されてきた。例えば本開特許第3796830号明細書には、非暗号テキスト・メッセージ(暗号化されていないメッセージ)の線形変換及び非線形変換を組合わせる積暗号システムが開示されている。これらの変換は、一意的な暗号キーを用いて行なわれ、このキーの関数になつている。暗号キーは、変換を制御することの他に、暗号システム内で種々のレジスタ代替及び部分的に暗号化されたデータのモジュロ2加算の制御も行なう。しかしながら、上記本開特許明細書には、キー経路指定器によるモジュロ2加算器への暗号キー・ビットの正確なマッピングの詳細や、代替機能ブロック内で実行される特別の非線形変換又は分散器(diffuser)によつて実行される暗

別の置換(permutation)の詳細(これらはすべて暗号処理操作の質に重大な影響を及ぼすものである)については、何ら開示されていない。暗号キーは、幾つかの小さなグループに分けられ、各グループに含まれる暗号キー・ビットは、暗号処理操作が繰返される度にシフトされる。各グループに含まれる暗号キー・ビットの数が比較的小ないため、各暗号キー・ビット・グループの重複す効率は、暗号処理操作の繰られた部分に限定される。これもまた、暗号処理操作の質に影響を及ぼすものである。更にこのシステムでは、暗号キー・ビットのみの関数として選択された2種類の代替機能ブロックだけが使用されているが、これも同様に暗号処理操作の質に影響を及ぼすものである。

上記のシステムに関連して、本開特許第3796830号明細書には、非暗号テキストのブロックがセグメント単位で処理されるような積暗号システムが開示されている。各セグメントは、暗号キーの一部に従つて、逐次に変換される。しかし

ながら、このシステムはその性能において直列式であるためにスループット速度が遅く、またもしこれを並列式に変更しようとするれば、そのハードウェアはかなり複雑になる。更に、前述のシステムと同様に、このシステムもまた同じような種類の代替機能ブロックのみに限定される。

本発明に従えば、任意に選ばれた1つの暗号キーの割割のもとに、32ビットのデータ・ブロックを暗号処理（暗号化又は解読）し得る暗号装置が提供される。この暗号装置は、全部で52個のデータ・ビットを有し且つ各々が4個のデータ・ビットより成る8個のセグメントに分けられたデータ・ブロックが、6個のデータ・ビットを各々有する8個のセグメントを構成する48個のデータ・ビットのブロックへ拡張されるような操作を実行することにより、暗号処理を行なう。このようなデータ・ビットの拡張は、8個の4ビット・セグメントの各々のエンド・データ・ビット、例えば最初の2ビットを二重にすることによつて達成される。8個の6ビット・セグメントとみなさ

れる拡張された48個のデータ・ビットは、任意に決められた順序に従つて選択された、8個の6ビット・暗号キー・ビット・セグメントとみなされる。8個の暗号キー・ビットとモジュロ2加算によつて組合せられる。モジュロ2加算の結果の8個の6ビット・セグメントは、8種類の非アフィン変換のための変換の引数を提供する。各変換操作においては、先行の6ビット・セグメントの二重にされたエンド・ビット及び置換された暗号キー・ビットのモジュロ2加算と、後続の6ビット・セグメントの二重にされたエンド・ビット及び別の置換された暗号キー・ビットのモジュロ2加算との結果として生じた6ビット・セグメントの2個のエンド・ビット（両端のビット）が解読されて、各々16個のエントリーを有する4個の検索テーブルのうちの1つが選択される。各エントリーは4ビットから成っている。次に、この6ビット・セグメントの残り4個のビットを解読することにより、選択された検索テーブルの16個の4ビット・エントリーの中の1つが選択される。各セ

グメントに対する変換操作に参与する検索テーブルは互いに異なっており、従つて、8種類の異なる変換操作が行なわれて、32ビットの代替セットを規定する8個の4ビット・セグメントが生じる。なお、本明細書において、「代替」とは成るビット・ブロックが別のビット・ブロックへ代えられることを意味し、「置換」とは取るビット・ブロック内においてビットの順序が変更されることを意味する。次に、この32ビットの代替セットは、任意に決められた置換による変換を受け、このような非線形置換及び線形置換の組合せにより、32ビットのデータ・ブロックの積ブロック暗号が生成される。

上述の積ブロック暗号処理操作は、暗号化及びキー・スケジュール関数によつて規定され得る積ブロック暗号処理アルゴリズムに従つて、16回繰返して実行される暗号化プロセスに使用される。かくして、暗号化プロセスにおいて、もし64ビットの入力メッセージ・ブロックが32ビットの1ブロックL及び32ビットの1ブロックRから成っていると、この入力メッセージ・ブロックは項LRで表わされる。また、もし暗号キー・ビットのブロックが暗号キーKEYから選ばれたらば、このブロックは項Kで表わされる。従つて、最後のものを除くすべての繰返しについては、入力がLRの時の出力は項L'K'で表わされる。これは、次のように定義され得る。

$$\begin{aligned} L' &= R \\ K' &= L \oplus f(R, K) \end{aligned} \quad (1)$$

上式において、 \oplus はビット毎のナジモ2加算（排他的オア）を換わり、各繰返し操作の間に、暗号キーKEYから暗号キー・ビットの異なるブロックKが選ばれる。最後の繰返しを除く各繰返

し後に出力が互換 (transpose) されるので、入力が L 及び R の最後の繰返しにおける出力は、次式で定義される項 $L'R'$ で表わされる。

$$\begin{aligned} L' &= L \vee f(R, K) \\ R' &= R \end{aligned} \quad (2)$$

更に、もしキー・スケジュール KS が 1 から 16 までの範囲にある整数 n 及び暗号キー KEY の関数として定義されるならば、暗号キー KEY からの暗号キー・ビットの置換された選択は、次式で定義される項 Kn によつて表わすことができる。

$$Kn = KS(n, KEY) \quad (3)$$

かくして、 L_{n-1} 及び R_{n-1} が各々 L 及び R の時に、もし L_0 及び R_0 が各々 L 及び R であり且つ L_n 及び R_n が各々 L' 及び R' であれば、 n が 1 から 15 までの範囲にある場合の繰返し操作の出力は次式で定義され得る。

$$\begin{aligned} L_n &= R_{n-1} \\ R_n &= L_{n-1} \oplus f(R_{n-1}, Kn) \end{aligned} \quad (4)$$

最後の繰返し操作の出力は互換されないで、 n が 16 の時の最後の繰返し操作の出力は次式で定義される。

$$\begin{aligned} L_n &= L_{n-1} \oplus f(R_{n-1}, Kn) \\ R_n &= R_{n-1} \end{aligned} \quad (5)$$

暗号化プロセスにおいては、 K_1 が最初の繰返しで使用され、 K_2 が 2 回目の繰返しで使用され、以下同様にして、最後の 16 回目の繰返しでは K_{16} が使用される。本発明に従う暗号化暗号処理アルゴリズムを利用するような暗号化プロセスの一例が第 8 図に示されている。

暗号関数 $f(R, K)$ は、選択関数と呼ばれる原始関数及び置換関数によつて定義され得る。かくして、もし 32 ビットのブロック R が 48 ビットのブロックへ拡張されるならば、拡張されたブロックは項 $E(R)$ で表わされる。この拡張されたブロック $E(R)$ は、任意に決められた置換に

従つて選択された暗号キー・ビットのブロック K とモジュロ 2 加算で組合わされ、8 個の 6 ビット・セグメント B_1, B_2, \dots, B_8 が生成される。これらのセグメントは、8 種類の異なる選択関数 S_1, S_2, \dots, S_8 に対する引数を構成する。従つて、モジュロ 2 加算は次のように定義され得る。

$$\begin{aligned} EXOR K &= B_1, B_2, B_3, B_4, B_5, B_6, \\ &B_7 \text{ 及び } B_8 \end{aligned} \quad (6)$$

各選択関数 S_i は、6 ビット・セグメント B_i を 4 ビット・セグメントへ変換し、このため 8 個の異なる選択関数は $S_1(B_1), S_2(B_2), S_3(B_3), S_4(B_4), S_5(B_5), S_6(B_6), S_7(B_7)$ 及び $S_8(B_8)$ として定義され得る。次に、8 個の選択関数の 8 個の 4 ビット・セグメントの出力は、32 ビットの単一ブロックへ結合される。この 32 ビット・ブロックは、置換関数 P によつて、次のように表わされる新しい 32 ビットのブロックへ交換される。

$$P(S_1(B_1), S_2(B_2), \dots, S_8(B_8)) \quad (7)$$

これが暗号関数 $f(R, K)$ を表わす。

本発明に従う暗号化暗号処理操作は、前と同じように暗号関数及びキー・スケジュール関数によつて規定され得る暗号化暗号処理アルゴリズムに従つて、16 回繰返しして実行される暗号化プロセスにも使用され得る。かくして、もし暗号化された 48 ビットの入力メッセージ・ブロックが、32 ビットの 1 ブロック L' 及び 32 ビットの 1 ブロック R' から成っていると、この暗号化された入力メッセージ・ブロックは項 L', R' で表わされる。従つて、入力が L', R' の最初の繰返しにおける出力は、互換された形で項 L, R で表わされ得る。これは、次のように定義することができる。

$$\begin{aligned} L &= L' \oplus f(K, K) \\ R &= R' \end{aligned} \quad (8)$$

この場合、各繰返し時に暗号キー KEY から選ばれた暗号キー・ビットの異なる順序のブロック K は暗号化操作の時に選ばれた順序とは反対の順序で

過される。最初の繰返しは、後続の各繰返しは最後のものを除いて反演され、従つて入力 L' 、 R' の後続の各繰返しにおける出力は、次の式で定義される項 L によつて表わすことができる。

$$\begin{aligned} L &= R' \oplus f(L', K) \\ R &= L' \end{aligned} \quad (9)$$

かくして、もし L_n 及び R_n が各々 L 及び R であり、 L_{n-1} 及び R_{n-1} が各々 L' 及び R' であれば、 n が16に等しい時の最初の繰返しの出力は次のように表わすことができる。

$$\begin{aligned} L_{n-1} &= L_n \oplus f(R_n, K_n) \\ R_{n-1} &= R_n \end{aligned} \quad (10)$$

最後の繰返しを除く各繰返しは出力が互換されるので、 n が15から1までの範囲にある場合の後続の各繰返しの出力は次の式で定義される。

$$\begin{aligned} L_{n-1} &= R_n \oplus f(L_n, K_n) \\ R_{n-1} &= L_n \end{aligned} \quad (11)$$

トのうちの所定のものを二重にすることによつて拡張されるような、また一組の暗号キー・ビット並びに一組のデータ・ビット及び二重にされたデータ・ビットに従つて制御される非線形変換機能を含むような積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、暗号処理されるべきデータ・ビットの一群の並列セグメントが、各セグメント中のデータ・ビットの所定のものを二重にすることによつて拡張されるような、また一組の暗号キー・ビットを含む一群の並列セグメント並びにデータ・ビット及び二重にされたデータ・ビットを含む一群の並列セグメントに従つて制御される一群の非線形変換機能を含むような積ブロック暗号処理プロセスを提供するにある。

特開 昭51-108701(5)

解読操作においては、最初の繰返しに K_{16} が使用され、2回目の繰返しに K_{15} が使用され、以下同様にして、16回目の繰返しでは K_1 が使用される。本発明に従う積ブロック暗号処理アルゴリズムを利用することによる解読プロセスの例が第8図に示されている。

従つて本発明の目的は、暗号キーの制御のもとにデータ・ブロックを暗号処理するための暗号装置を提供するにある。

本発明の他の目的は、暗号キーの制御のもとにデジタル・データを暗号処理するための積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、暗号キー及びデジタル・データに従つて制御される非線形変換を含む積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、多数対1の非線形変換を含む積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、暗号処理されるべきデータ・ビットのブロックが、これらのデータ・ビッ

前にも解れたように、データ処理ネットワークの内部においては、データの傍受又は変更や、記憶媒体の物理的な取外しに対して、ネットワークを物理的に保護することは極めて困難である。この問題は、データが通信線を介して処理装置と送受信制御ユニット又は送受信本との間でやりとりされる場合、非常に長いケーブル接続を介して制御ユニットと端末即ち入出力装置との間でやりとりされる場合、又は移動可能な記憶媒体が設置されている場合において最も顕著に生じる。このような状況のもとでデータの秘密保護を達成し、プライバシーを守るための1つの手段として、ネットワーク内の重要な場所には暗号装置が設置される。送信局においては、暗号化モードで動作する暗号装置によつて非暗号データが暗号化された後、この暗号化データが受信局の方へ伝送される。受信局側では、解読モードで動作する暗号装置を用いて、伝送されてきた暗号化データを解読することにより、元の非暗号データが得られる。受信局及び送信局の役割が反対になった時、即ち今まで

受信局として働いていたところが送信局になり且つ送信局として働いていたところが受信局になった時には、各々の局に設置されている暗号装置も同様に今までとは反対のモードで動作される。第1図は、代表的なデータ送受ネットワークにおける暗号装置の設置場所を例示したものである。第1図の例では、暗号装置は無い丸印の部分に設置されている。

第2図は、8バイトから成る64ビットのデータ・ワードDW即ちデータ・メッセージ・ブロックを暗号化又は解読するための暗号装置を示したものである。図において、太い実線の途中にある丸印で囲まれた数字は、各々の母線を介して送られるビットの数を表わしている。各バイトは8個のデータ・ビットを含んでいる。メッセージ・ブロックのデータ・バイトは、データ・バス・インを介して、時に1つずつ逐次に暗号装置へ印加され、従つて、64ビットのメッセージ・ブロックを完全に転送するには、8サイクルを必要とする。暗号装置に受信された各バイトは、通常の交差配

線ボックス50(以下、Pボックスという)によつて実行される初期変形変換(ビント順序の変換)を受ける。次いで、各々の置換されたデータ・バイトは2つに分割されて、偶数番目のビット0、2、4及び6が上部入力ボックス(以下、UIBと略す)100に印加され、奇数番目のビット1、3、5及び7が下部入力ボックス(以下、LIBと略す)150に印加される。UIB100及びLIB150は、直列-並列変換を実行し、従つて、メッセージ・ブロックの8バイトが受信された後に、UIB100はメッセージ・ブロックの第1半分の32ビットを上部データ・レジスタ(UDR)200へ並列に供給し、一方LIB150はメッセージ・ブロックの残り32ビットを下部データ・レジスタ(LDR)250へ供給する。

64ビットのメッセージ・ブロックが受信されて、UIB100及びLIB150へバンプアップされている時に、各々が7個のキー・ビント及び1個のパリティ・ビントを含む8個のキー・バイトを供給する64ビットの外部レジスタから暗号キ

ーが入力される。この暗号キーの各暗号キー・バイトは、8番目のビット即ちパリティ・ビットを除いて、一時に7ビット・バイトずつキー・バス・インを介して暗号装置へ印加される。この場合も、暗号キーを完全に転送するには、8サイクルを必要とする。上述のメッセージ・ブロックと同様に、暗号装置に受取られた各暗号キー・バイトもPボックス50による初期変換を受け、この後、暗号キーの各々の置換されたバイトは2つに分割されて、各7ビット・バイトの最初の4ビットが上部キー・レジスタ(UKR)350へ印加され、残りの3ビットが下部キー・レジスタ(LKR)400へ印加される。UKR350及びLKR400は各々28個の段を有し、UKR350の最後の段がLKR400の25番目の段に接続されている。UKR350及びLKR400は共に直列-並列変換を行ない、8個の7ビット・バイト(各々が8ビットを含む7個のグループと考えられる)が逐次に受取られている間に、これら7グループのうちUKR350の段U、B及び

16へ各々逐次に受取られた8ビットより成る3グループと、LKR400の段0、8及び16へ各々逐次に受取られた8ビットより成る3グループとが、各々3個の並列8ビット・グループへ変換される。これら2つの3グループは、UKR350及びLKR400における24ビットの2つの並列グループとみなされ得る。7個の8ビット・グループの残りのグループは、UKR350の段24へ逐次に受取られる。UKR350の最後の段LKR400の段24とが接続されているので、UKR350へ逐次に受取られた残りの8ビット・グループの最初の4ビットは、LKR400へ送られて、その段の4段において4ビットの並列部分グループへ変換され、次の4ビットはUKR350の最後の4段において4ビットの並列部分グループへ変換される。かくして、UKR350及びLKR400は、各々が28ビットの2個の並列グループとみなされる暗号キーを含む。

この時点においては、メッセージ・ブロックの第1半分及び第2半分が各々UIB200及びL

DR 250へ搬送され、そしてUKR 350及びLKR 400には暗号キーがロードされているが、一旦UKR 350及びLKR 400へロードされると、これから2つのレジスタ間の繰移はこれ以上使用されず、UKR 350及びLKR 400は、各々28ビットの独立したシフト・レジスタとして動作する。暗号化プロセスにおいては、UKR 350及びLKR 400の暗号キー内各が1ビット位置だけ単回シフトされた後に、16回の繰移し操作が連続的に実行される。暗号化プロセスの繰移し操作（最初のものを除く）の際に、UKR 350及びLKR 400の暗号キー内各は1又は2ビット位置だけシフトされる。各レジスタは所定のシフト距離に従って、暗号化プロセスの間に常に28ビット位置シフトされるので、この手続は暗号キー・ビットの適切な並びを確保に行わせるものである。

暗号化操作の最初の繰移しにおいては、ULM 200に与えられるメッセージ・ブロックの第1半分（32個のデータ・ビット）を読み、これらは各

ものと与えられる生成された48個のデータ・ビットと、同じく8個の6ビット・セグメントを繰移するものと与えられる生成された48個の暗号キー・ビットとを並列的に組合わせて、8個の非アフィン変換機能ボックス（以下、8ボックスという）550～564のための変換の引数を提供する8個の6ビット・セグメントを出力する。各8ボックスは非線形変換を実行する。各8ボックスにおいては、先行の6ビット・データ・セグメントの二進にされた1エンド・ビット及び生成された1暗号キー・ビットのモジュロ2加算と、後続の6ビット・データ・セグメントの二進にされた1エンド・ビット及び別の生成された1暗号キー・ビットのモジュロ2加算との結果として生じた6ビット・セグメントの2エンド・ビットが形成されて、8ボックス内の記憶専用記憶装置（メモリ）に与えられる4個の16エントリ変換テーブルのうちの1つが選択される。各エントリは4ビットから成っている。次に、選択された変換テーブルにおける16個の6ビット・エントリ

々4個のデータ・ビットより成る8個のセグメントとみなされる）は、各々6個のデータ・ビットを含む8個のセグメントを繰移する48個のデータ・ビットへ提供される。この生成は、8個の4ビット・セグメントの各々のエンド・ビットを二進にすることによつて達成される。生成された48個のデータ・ビット（8個の6ビット・セグメントを繰移するものと与えられる）は、8個のモジュロ2加算器500～514へ並列的に印加される。各モジュロ2加算器は6個の非恒等的オア回路より成っている。これと同時に、56個の暗号キー・ビットのうち、UKR 350から選択された24個のキー・ビット及びLKR 400から供給された24個のキー・ビットより成る48個の所定の暗号キー・ビットは、Pボックス450において繰移距離（一定）された後、8個の6暗号キー・ビット・セグメントとして、8個のモジュロ2加算器500～514の非恒等的オア回路へ並列的に印加される。8個のモジュロ2加算器500～514は、8個の6ビット・セグメントを繰移する

のうちの1つが、供給された6ビット・セグメントの残り4ビットを繰移することにより選択される。8個の8ボックスは並列的に成っており、従つて8個の6ビットの生成された変換結果が実行されて、32ビットより成る1組の代価を決定する8個の4ビット・セグメントが与えられる。次に、これらの32ビットはPボックス600において、与えられた変換による繰移距離を受ける。このような非線形変換及び繰移距離の組合わせにより、メッセージ・ブロックの第1半分に対する32ビットの複ブロック暗号が生成される。この複ブロック暗号は、モジュロ2加算器650～664へ印加される。ULM 250にあるメッセージ・ブロックの第2半分の32データ・ビットもモジュロ2加算器650～664へ印加される。モジュロ2加算器650～664は、メッセージ・ブロックの第1半分に対するPボックス600からの32ビットの複ブロック暗号に従つて、ULM 250からのメッセージ・ブロックの残り32ビットを繰移する。この結果、メッセージ・プロ

ブロックの宛先された第2半分を渡す新しい32ビットの組を構成する8個の4ビット・グループが与えられる。メッセージ・ブロックの宛先された第2半分の32ビットは、メッセージ・ブロックの第1半分を言んでいたUDR200へ追加され、これと同時に、メッセージ・ブロックの第1半分は、第2半分を言んでいたLDR250へ追加される。かくすることにより、メッセージ・ブロックの第1半分及び第2半分の互換が達成される。

暗号化プロセスの次の搬送し時においては、UKR550及びLKR400に記憶されている暗号キーが、所定のシフト引延に従ってシフトされ、これにより新しい暗号キー・ビットの組が供給される。次に、UKR200に記憶されているメッセージ・ブロックの宛先された第2半分の32ビットが、同様のブロック暗号操作において、新しい暗号キー・ビットの組と共に使用される。モジュロ2加算器650～664は、このブロック暗号処理の結果に応じて、LDR250に記憶されているメッセージ・ブロックの第1半分の3

2ビットを宛先する。この宛先された第1半分の32ビットは、メッセージ・ブロックの宛先された第2半分の32ビットを配接していたUR200へ追加され、これと同時に、宛先された第2半分の32ビットは、メッセージ・ブロックの第1半分の32ビットを配接していたLUR250へ転送される。

暗号化の搬送しを続く後続の各搬送し操作時においては、UKR550及びLKR400にある暗号キー・ビットは、所定のシフト引延に従ってシフトされ、LUR250に記憶されているメッセージ・ブロックの宛先された半分の32ビットのブロック暗号処理に従って再宛先され、そしてモジュロ2加算器650～664からの再宛先された半分の、既に宛先された他の半分の半分を記憶していたUDR200へ追加され、これと同時に、この他の半分の半分はLDR250へ転送されて、メッセージ・ブロックの第1半分及び第2半分の互換が行

なわれる。

暗号の搬送し操作時には、UKR550及びLKR400にある暗号キー・ビットは、所定のシフト引延に従って連続シフトされて、宛先された暗号の暗号キー・ビットの組が生成され、LUR250に記憶されている32ビットの宛先された半分の宛先する暗号の再宛先が、UDR200に記憶されている前に宛先された半分の32ビットのブロック暗号処理に従って実行される。しかしながら、モジュロ2加算器650～664からの宛先された第2半分及びUDR200に記憶されている前に宛先された半分の互換は互換されることはなく、元のメッセージ・ブロックに対する64ビットの暗号化されたブロックを構成する。16回目の搬送し後、UDR200の32ビットの内容及びモジュロ2加算器650～664の32ビットの出力（これらは一緒になつて、暗号化されたデータ・メッセージ・ブロックを渡す）は、上部出力バス（UOB）700及び下部出力バス（LOB）750へ各々転送される。次の

で、UOB700に記憶されている暗号化された4個の8ビット・バイトのデータ及びLOB750に記憶されている暗号化された4個の8ビット・バイトのデータで構成される64ビットの暗号化されたデータ・ブロックは、8ビット・バイト単位の並列一直列変換を受け、一時11バイトずつPボックス800へ転送される。64ビットの暗号化されたデータ・メッセージ・ブロックを完全に転送し終るためには、8サイクルが必要である。暗号化されたデータの各バイトは、受信局への伝送のために、暗号化されたデータ・ビットをデータ・バス・アクトの適切なビット組へ搬送すべく、Pボックス800において暗号の暗号暗号を受け

る。受信局においては、同じ暗号キーの制御のもとに同様の16回の搬送し操作を実行することにより、64ビットの暗号化されたデータ・メッセージ・ブロックが解放される。しかしながら、暗号化プロセスの時とは異なり、解放プロセスに先立つUKR550及びLKR400の暗号キー内容

の事前シフトは行なわれない。解読プロセスの繰返し操作（最初のものを除く）においては、UKR350及びLKR400の暗号キー内容は、暗号化プロセスの時と同様に、所定のシフト計画に従つて、1又は2ビット位置だけシフトされるが、暗号化プロセスを逆にして、その時実行されたすべての繰返しを元に戻すため、暗号キーのシフト方向は暗号化プロセスの時とは反対にされる。かくすることにより、元の64ビットのメッセージ・ブロックと同一のメッセージ・ブロックが再生される。また、解読プロセスの繰返し操作中に、UKR350及びLKR400の暗号キー内容は27ビット位置シフトされる。従つて、UKR350及びLKR400は共に28ビットのシフトレジスタであるから、解読プロセスの終了において、UKR350及びLKR400の暗号キー内容は、既に1ビット位置だけ繰返シフトされる。この結果、暗号キーは所定のシフト計画に従つて、UKR350及びLKR400において完全に1回シフトされることになり、解読プロセスの各

繰返し操作における暗号キー・ビットの適切な並びを確保に行なわせると共に、別の解読プロセスに対する準備ができる。

本特開に従う暗号装置の詳細は第3a-3j図に示されており、次にこれらの図面並びに第7a図及び7b図のタイミング図を参照して、より詳細な説明を行なうが、その前に、本発明の暗号装置で用いられるラッチ回路の具体例について、第4図を参照して説明しておく。ラッチ回路10は、4相のタイミング・クロックで作動されるダイナミックPBT回路によつて実現することができる。各クロック相は、例えば250ナノ秒の持続時間を有しており、この場合、完全な1クロック・サイクルは1マイクロ秒になる。基本ラッチ回路は、正電源と接地28との間に接続され、ゲート電極に施されクロック信号φ1が印加される素子22と、素子28及び29の間に並列的に接続され、各々のゲート電極に入力D3及びG3並びに入力D4及びG4が印加される2対の素子23及び24並びに25及び26と、素子29及び26の間に接続され、

ゲート電極に繰返しクロック信号φ2が印加される素子30と、正電源及び接地間に接続され、各々のゲート電極に繰返しクロック信号φ3、素子28及び29に繰返しクロック信号φ4に接続された3個の直列接続素子32、33及び34とを有している。素子22及び23間の接続点は、ラッチ回路10の入力素子36へ接続されると共に、素子25のゲート電極へフィードバック接続されて、入力D4を与える。回路内の繰返シ容量性素子及び絶縁容量性素子は、一まとめにして容量性素子31及び35として示されている。素子23及び24並びに25及び26はアシッド回路として、素子28はドット・オフ手段として、そして素子30はインバータとして各々働く。

次に、第5図をも参照して、第4図のラッチ回路10の動作について説明する。ラッチ回路10が最初"0"状態にあるものとする、クロック信号φ1が印加されて、素子22がターン・オンされた時には、素子28は正電源の電位まで充電される。この時、クロック信号φ2は印加されてい

ないので、素子30はカント・オフ状態に保たれており、従つて素子28の充電は継続に行なわれる。次に、クロック信号φ2が印加されると、素子28上の電荷は、入力D3及びG3又は入力D4及びG4へ印加される信号に応じて、そのまま保たれるか又は放電される。ラッチ回路10は0状態にあるものと仮定しているので、入力D4には低レベルの信号が印加されて、素子25を非過渡に保ち、また入力G4にも低レベルの信号が印加されて、素子26を非過渡に保つ。従つて、素子25、26及び30を介する放電路は働かない。素子23及び24を含む放電路に関しては、もし入力D3に"1"ビット（高レベル信号）が印加され、且つこれと同時に入力D3にゲート信号（高レベル信号）が印加されると、素子23及び24は共に導通して、素子30を介する放電路を形成し、その結果、素子28上の電荷は接地電位の方へ放電される。これに対し、入力D3に"0"ビット（低レベル信号）が印加されていると、たとえ入力D3にゲート信号が印加されても、クロックφ2

の間素子25は非導通に保たれるので、素子28から素子24及び30を介して接地に至る放電経はあらず、従つて高レベルの信号が素子28上に保持される。

次に、素子32のゲート電極へクロック信号φ3が印加されると、この時はまだクロック信号φ4が印加されていないので、素子34は非導通に保たれており、従つて素子36は正電極の電位まで充電される。次に、素子34のゲート電極へクロック信号φ4が印加されると、素子36上の電荷は、素子28上の信号のレベルに応じてそのまま保持されるか又は放電される。もし素子28上に“1”ビットのデータ入力を設けず低レベルの信号が存在すると、クロックφ4の間素子33は非導通に保たれ、従つて素子36から素子34を介して接地に至る放電経はあらず、素子36上には“1”ビットの存在を要する高レベルの信号が保持される。入力D3に新しい入力信号が印加されない限り、ゲート信号D3は低レベルに立つてゲート信号D4は高レベルに保たれるので、ラッチ回路10が“1”

ビット状態にセットされた後は、素子25及び26のゲートに高レベルの信号が印加され、従つて次の2クロック時に素子25、26及び30を介する放電経が働いて、素子28を低レベルに保つ。これにより素子33は非導通に保たれるので、素子34を介する放電経は働かず、かくして素子36は、次の新しいデータ入力が印加されて、第5図に示されるようなゲート信号D3及びD4が印加されるまで高レベルに保たれる。これに對して、“0”ビットのデータ入力の結果として、素子28上に高レベルに信号が存在すると、クロックφ4の印加時に素子33が導通して、素子34を介する放電経を形成し、その結果、素子36上には“0”ビットの存在を要する低レベルの信号が保持される。この場合、入力D4に低レベルの信号が印加されることとなるので、素子25は非導通に保たれ、従つて素子28に対する放電経は形成されない。このため、素子28上には電荷即ち高レベルの信号が保持される。この状態はまた素子33を導通状態に保ち、これにより素子34を介する放電経が

経通されて、素子36を低レベルに保つ。かくして、ラッチ回路10の出力において有効データが確実に得られる。

ラッチ回路10が“1”状態にある場合にも、クロック・サイクルは素子22へのクロック信号φ1の印加によつて開始される。前と同様に、素子22はクロックφ1の印加により導通して、素子28を正電極の電位まで充電させる。次に、クロック信号φ2が印加されると、素子28上の電荷は、入力D3及びD3又は入力D4及びD4に印加されている信号のレベルに応じて、そのまま保持されるか又は放電される。もし入力D3に“1”ビットのデータが印加されると、素子28上には低レベルの信号が保持され、一方入力D3に“0”ビットのデータが印加されると、高レベルの信号が保持される。次に、素子32のゲート電極へクロック信号φ3が印加されると、この時クロック信号φ4がまだ印加されていないので、素子34は非導通に保たれ、従つて、素子36は正電極の電位まで充電される。次に、素子34のゲート電極へ

クロック信号φ4が印加されると、素子36上の電荷は、素子28上の信号のレベルに応じて、そのまま保持されるか又は放電される。前に説明したように、 “1”ビットのデータ入力の結果として、素子28上に低レベルの信号が存在すると、素子36上には高レベルの信号が保持されて、“1”ビットの存在を要し、一方、“0”ビットのデータ入力の結果として、素子28上に高レベルの信号が存在すると、素子36上には低レベルの信号が保持されて、“0”ビットの存在を要する。

ラッチ回路10は、入力D1及びG1に各々接続された素子18及び19を使用することによつて、2ウェイ入力へ拡張することができ、更に他の入力D2及びD2に各々接続された素子20及び21を使用することによつて、3ウェイ入力へ拡張することもできる。以下で詳細に説明する本発明の幾何例においては、1ウェイ入力、2ウェイ入力又は3ウェイ入力のラッチ回路が必要に応じて使用される。

まず素子30図に示されるように、8ビットから

る64ビットのデータ・メッセージ・ブロックは、データ・バス・インを介して一時に1バイトずつPボックス50へ印加される。各バイトはPボックス50において初期置換を受け、偶数番目(0, 2, 4, 6)のデータ・ビットより成る組及び奇数番目(1, 3, 5, 7)のデータ・ビットより成る組に分割される。偶数番目の組はUIB100へ送られ、一方、奇数番目の組はLIB150へ送られる。UIB100は4個の8段シフト・レジスタ0UIB, 1UIB, 2UIB及び3UIBで構成され、LIB150も同様に4個の8段シフト・レジスタ0LIB, 1LIB, 2LIB及び3LIBで構成される。第3a図には、第1シフト・レジスタ0UIBの最初及び最後の段のみが詳細に示されているが、他のシフト・レジスタもこれと同じ構造である。

第7a図のタイミング図をも併せて参照するに、サイクル0において、1つの有効データ・バイトがPボックス50を介して、UIB100及びLIB150へ印加されている時に、タイミング及

び制御信号60からLIB(G3)線及びLIB(G4)線へ信号が印加されて、最初の8ビット・バイトが、UIB100及びLIB150の各シフト・レジスタの最初の段のランチャ(例えば102)へロードされる。メッセージ・ブロックの残りの8ビット・バイトは、次のサイクル1から7までの間に、一時に1バイトずつUIB100及びLIB150へ印加される。この場合、バイトの各ビットは、各シフト・レジスタの最初の段(G3)へ印加される。LIB線及びLIB線上の信号は、シフト・レジスタの各段へ印加されるので、サイクル1乃至7の各々において、データ・ビットは各シフト・レジスタ内で1ビット位置ずつシフト・ダウンされ、従つてサイクル7の終了時には、UIB100及びLIB150は、供給されたデータ・メッセージ・ブロックを半分ずつロードされている。UIB100及びLIB150は逐列・逐列置換を実行し、その結果、UIB100及びLIB150へ逐次供給された8バイトのメッセージ・ブロックは、これらの出

力において、各々32ビットより成る2つのグループ(メッセージ・ブロックの第1半分及び第2半分)へ形成される。

次に、第3b, 3c及び3d図を参照するに、64ビットのメッセージ・ブロックがUIB100及びLIB150へ受取られて、さらにハンプアップされている間に、64ビットの外部レジスタからキー・バス・インを介して、暗号キーが一時に7ビット・バイトずつPボックス300へ逐次印加される。各7ビット・バイトはPボックス300で初期置換を受け、最初の4キー・ビット及び残りの3キー・ビットへ分割される。最初の4キー・ビットはUKR350へ印加され、一方、残りの3キー・ビットはビット位置を逆にしてLKR400へ印加される。UKR350は5個の8段シフト・レジスタ0UKR, 1UKR及び2UKR並びに1個の4段シフト・レジスタ3UKRで構成され、同様にLKR400も3個の8段シフト・レジスタ0LKR, 1LKR及び2LKR並びに1個の4段シフト・レジスタ3LKRで

構成される。シフト・レジスタ0UKRの4段目のランチャ390の出力は、シフト・レジスタ3LKRの1段目のランチャ402の入力に接続されている。第3b図に詳細に示されているように、8段シフト・レジスタ0UKRの第1段は3ウェイ入力ランチャ352で構成され、他の段は第2段及び最後の段のランチャ354及び366の如き2ウェイ入力ランチャで構成される。8段シフト・レジスタ1UKR及び2UKRもこれと同じ構成である。4段シフト・レジスタ3UKRについては、第3c図に示されるように、第1段は3ウェイ入力ランチャ384で構成され、他の各段はランチャ390の如き2ウェイ入力ランチャで構成される。第3c及び3d図にブロック図で簡単に示されているLKR400の8段シフト・レジスタ0LKR, 1LKR及び2LKRは、UKR350の対応する8段シフト・レジスタ0UKR, 1UKR及び2UKRと同じ構成を有している。第3d図に示される4段シフト・レジスタ3LKRについては、その第1段は、シフト・レジスタ3UKRの最終

設のラッチ390の出力に接続された3ウェイ入力ラッチ402で構成され、他の各段は最終設のラッチ408の如き2ウェイ入力ラッチで構成される。かくして、UKR350及びLKR400の組合わせは、暗号キー・ワードのキー・ビットを記号するための7個の8段シフト・レジスタから成っているものとみなすことができる。

次に、第7図を参照して、暗号キーのロード動作について説明する。サイクル0において有効暗号キー・ビットがPホックス300を介してUKR350及びLKR400へ印加される時に、シフト・レジスタ0UKR、1UKR、2UKR、3UKR、0LKR、1LKR及び2LKRの第1段に接続されたLDK(G3)線及びLDK(G4)線へ信号が印加され、これにより最初の7ビット・キー・ビットがUKR350及びLKR400の7個の各シフト・レジスタの第1段、例えば入力ラッチ552、568及び584などへロードされる。

サイクル1においては、暗号キーの2番目の7

ビット・バイトが、UKR350及びLKR400の7個のシフト・レジスタの第1段へロードされる。これと同時に、各第1段の以前の内容即ち暗号キーの最初の7ビット・バイトは、シフト・レジスタ0UKR、1UKR、2UKR、3UKR、0LKR、1LKR及び2LKRの第2段に接続されているSR(G3)線及びLDK線への信号印加により、各々1ビット位置だけシフト・ダウンされる。各段のラッチ内部の分解時間(resolve time)は、前段のラッチの出力に変化が生じる前にシフト動作を行なわせるのに十分なものである。

サイクル2においては、暗号キーの3番目の7ビット・バイトが、UKR350及びLKR400の7個のシフト・レジスタの第1段へロードされる。これと同時に、第1段及び第2段の以前の内容即ち暗号キーの2番目及び最初の7ビット・バイトは、シフト・レジスタ0UKR、1UKR、2UKR、3UKR、0LKR、1LKR及び2LKRの第2段及び第3段に接続されているSR

線及びLDK線への信号印加により、各々1ビット位置だけシフト・ダウンされる。

サイクル3及び4においては、暗号キーの4番目及び5番目の7ビット・バイトが、7個のシフト・レジスタの第1段へ逐次にロードされ、これと同時にその内容は1ビット位置ずつシフト・ダウンされる。しかしながら、シフト・レジスタ3UKRの最終段にあるビットは、サイクル4においてシフト・レジスタ3LKRの第1段へシフトされる。該段のサイクル5、6及び7においては、暗号キーの残りの7ビット・バイトが、シフト・レジスタ0UKR、1UKR、2UKR、3UKR、0LKR及び2LKRの第1段へ一時1ビットずつロードされる。LDK線及びLDK線上の信号は、各シフト・レジスタの第1段へ印加される。一方、SR線及びLDK線上の信号は、各シフト・レジスタの残りの段へ印加されるので、サイクル5、6及び7の各々においては、暗号キー・ビットは1ビット位置ずつシフト・ダウンされ、従つてサイクル7の終了時には、UKR350及

びLKR400は暗号キーの第1半分及び第2半分を各々ロードされている。

暗号キーのロード動作においては、UKR350及びLKR400は逐列-逐列動作を行ない、従つてUKR350及びLKR400に記憶されている暗号キーの8個の7ビット・バイトは、各々28ビットより成る2組の逐列グループとして与えることができる。下記の表1及び表2は、UKR350及びLKR400へ暗号キーをロードする際のキー・ビットのマッピングの様子を示したものである。

表 1

UKRに対する番号マッピング

UKRのビット位置	番号マッピング
UKR 0 - UKR 7	56 48 40 32 24 16 8 0
UKR 8 - UKR 15	57 49 41 33 25 17 9 1
UKR 16 - UKR 23	58 50 42 34 26 18 10 2
UKR 24 - UKR 27	59 51 43 35

表 2

LKRに対する番号マッピング

LKRのビット位置	番号マッピング
LKR 0 - LKR 7	62 54 46 38 30 22 14 6
LKR 8 - LKR 15	61 53 45 37 29 21 13 5
LKR 16 - LKR 23	60 52 44 36 28 20 12 4
LKR 24 - LKR 27	27 19 11 3

図3に示されるUDR200及びLDR250は、各々32ビットのラッチ0UDR~31UDR及び0LDR~31LDRで構成される。第7図に示されるように、マイクログラフに於いてIH及びLDR線へ信号が印加され、これによりU1H100にある32個のデータ・ビット及びL1B150にある32個のデータ・ビットが、各々UDR200及びLDR250へ並列的に転送される。メッセージ・ブロックの64ビットは、下記の表3及び表4に示される如く、UDR200及びLDR250へ分配される。

表 3

UDRに対するデータマッピング

UDRのビット位置	データ・ビット
UDR 0 - UDR 7	56 48 40 32 24 16 8 0
UDR 8 - UDR 15	58 50 42 34 26 18 10 2
UDR 16 - UDR 23	60 52 44 36 28 20 12 4
UDR 24 - UDR 31	62 54 46 38 30 22 14 6

表 4

LDRに対するデータマッピング

LDRのビット位置	データ・ビット
LDR 0 - LDR 7	57 49 41 33 25 17 9 1
LDR 8 - LDR 15	59 51 43 35 27 19 11 3
LDR 16 - LDR 23	61 53 45 37 29 21 13 5
LDR 24 - LDR 31	63 55 47 39 31 23 15 7

第7図に示されるように、LDR線へのこれ以上信号は印加されない。従つて、シフト・レジスタ3UKRの最終段のラッチ390からシフト・レジスタ3LKRの第1段のラッチ402に至る間は以後使用されず、これらの間では同例なるビット転送も行なわれない。シフト・レジスタ3UKRの最終段のラッチ390の出力は、シフト・レジスタ0UDRの第1段のラッチ352に転送され、シフト・レジスタ3LKRの最終段のラッチ408の出力は、シフト・レジスタ0LKRの第1段のラッチ(図示せず)に転送されているので、UKR350及びLKR400は、各々独立した28ビットのシフト・レジスタと考えることができる。UKR350及びLKR400に転送されている番号マッピング・ビットは、番号化プロセスに先立つて1ビット位相ずつてシフト・アンプされる。この場合、UKR350の第1段のラッチ352に転送されていたビットは、UKR350の最終段のラッチ390へ循環シフトされ、同様に、LKR400の第1段のラッチに転送さ

暗号化のシフト計画

暗号化 シフト	暗号化 (シフト・アップ)		暗号化 (シフト・ダウン)
	(暗号シフト)	1	
1			
2	1		1
3	2		2
4	2		2
5	2		2
6	2		2
7	2		2
8	2		2
9	1		1
10	2		2
11	2		2
12	2		2
13	2		2
14	2		2
15	1		1
16			
(暗号シフト)			

れていたビットは、LKR400の最終段のラン
チ408へ循環シフトされる。このような循環シ
フトは、サイクル8において、UKR350及び
LKR400のすべての段にわたって行な
われ、SL及びLDKへの信号を印刷することにより行な
われる。各フロッグの出力は前段のランチへ接続さ
れており、従って、SL及びLDKへの信号
印刷により、各ランチから前段のランチへキー・
ビットが転送される。例えば、これらの信号印刷
によつてランチ354のビット内容をランチ35
2へ有効にシフトさせるため、ランチ354の出
力UKR1はランチ352の1入力に接続されて
いる。同様に、ランチ352のビット内容をラン
チ390へ有効にシフトさせるため、ランチ35
2の出力UKR0はランチ390の1入力に接続
されている。暗号化プロセスの開始前に行なわれ
るこのような暗号キー・ビットの事前シフトは、
暗号化プロセスの最初の繰返しにおけるキー・ビ
ットの適切な並びを確保に用いられるものである。暗号
化プロセスに入ると、UKR350及びLKR4

00にある暗号キー・ビットを共に27ビット位
置シフトさせるため、最初の繰返しを除く各繰
返しの間に、UKR350及びLKR400は1又
は2ビット位置ずつシフトアップされる。UK
R350及びLKR400は共に28ビットのシ
フト・レジスタであるから、これらに記憶されて
いる暗号キー・ビットの28ビット、即ち、1番
目シフト及び暗号化プロセスにおける27シフト
は、暗号化プロセスの開始時と同様、繰返し動作
の間に暗号キー・ビットを適切に並列させるもの
である。下記の表5は、暗号キーに對する所定の
シフト計画を示したものである。

特開 51-108701(14)

暗号化のシフト計画

暗号化 開始位置	暗号化 (シフト・アップ)		暗号化 (シフト・ダウン)
	(第1シフト)	1	
1			
2	1		1
3	2		2
4	3		3
5	2		2
6	2		2
7	2		2
8	2		2
9	1		1
10	2		2
11	2		2
12	2		2
13	2		2
14	2		2
15	2		2
16	1		1
		(第2シフト)	1

れていたビットは、LKR400の最終段のランナ352へ復元シフトされる。このような事前シフトは、サイクル8において、UKR350及びLKR400のすべての段に施されているSL及びLDK段への信号を印加することにより行なわれる。各ランナの出力は前段のランナへ接続されており、従って、SL段及びLDK段への信号印加により、各ランナから前段のランナへキー・ビットが転送される。例えば、これらの化号印加によつてランナ354のビット内容をランナ352へ有効にシフトさせるため、ランナ354の出力UKR1はランナ352の1入力に接続されている。同様に、ランナ352のビット内容をランナ390へ有効にシフトさせるため、ランナ352の出力UKR0はランナ390の1入力に接続されている。暗号化プロセスの開始期に行なわれるこのような暗号化キー・ビットの事前シフトは、暗号化プロセスの最初の繰返しにおけるキー・ビットの適切な並びを確保に使用するものである。暗号化プロセスに入ると、UKR350及びLKR4

00にある暗号化キー・ビットを共に27ビット位置シフトさせるため、最初の繰返しを既く各繰返しの間に、UKR350及びLKR400は1又は2ビット位置ずつシフト・アップされる。UKR350及びLKR400は共に28ビットのシフト・レジスタであるから、これらに記憶されている暗号化キー・ビットの28ビット、即ち、1事前シフト及び暗号化プロセスにおける27シフトは、暗号化プロセスの開始時と同様、繰返し動作の間に暗号化キー・ビットを適切に連列させるものである。下記の表5は、暗号化キー・ビットに対する所定のシフト計画を示したものである。

特開昭51-10870(14)

表5中の"1"は、UKR350及びLKR400における1ビット位置のシフトを要し、"2"は2ビット位置のシフトを要す。

暗号化プロセス

本発明に従う暗号装置を用いる暗号化プロセスは、16回の繰返し操作によつて、データ・ビットのメッセージ・ブロックを暗号化する。

UKR350及びLKR400にある暗号キー・ビットの最初シフトは、暗号化プロセスの開始時に、サイクル8において実行される。これは、UKR350及びLKR400のすべての鍵にかけられているS L鍵及びL D K鍵へ最初の信号を加算することによつて行なわれ、暗号キーは1ビット位置だけシフト・アップされる。この結果、サイクル8の終了時には暗号化プロセスの最初の繰返し操作のための暗号キー・ビットの最初の組が与えられる。暗号化プロセスの最初の繰返し操作は、サイクル9及び10で実行され、UKR350にある28個の最初シフトされた暗号キー・

ビットのうちの24ビット及びLKR400にある28個の最初シフトされた暗号キー・ビットのうちの24ビットをPボックス450で図形置換することにより開始される。Pボックス450は、下記の暗号キー・ビットのマッピングを示す表6及び7に従つて、UKR350及びLKR400からの48ビットの任意に決められた置換を行なう。

表 6

暗号キー・ビットの置換マップ

ビット番号	置換されたビット番号
UKR 0	UKR 13
UKR 1	UKR 16
UKR 2	UKR 10
UKR 3	UKR 23
UKR 4	UKR 0
UKR 5	UKR 4
UKR 6	UKR 2
UKR 7	UKR 27
UKR 8	UKR 14
UKR 9	UKR 1
UKR 10	UKR 20
UKR 11	UKR 9
UKR 12	UKR 27
UKR 13	UKR 14
UKR 14	UKR 19
UKR 15	UKR 11
UKR 16	UKR 7
UKR 17	UKR 25
UKR 18	UKR 7
UKR 19	UKR 15
UKR 20	UKR 8
UKR 21	UKR 26
UKR 22	UKR 10
UKR 23	UKR 17
UKR 24	UKR 12
UKR 25	UKR 17
UKR 26	UKR 12
UKR 27	UKR 1

表 7

暗号キー・ビットの置換マップ

ビット番号	置換されたビット番号
LKR 0	LKR 12
LKR 1	LKR 23
LKR 2	LKR 2
LKR 3	LKR 8
LKR 4	LKR 18
LKR 5	LKR 26
LKR 6	LKR 1
LKR 7	LKR 11
LKR 8	LKR 22
LKR 9	LKR 16
LKR 10	LKR 4
LKR 11	LKR 19
LKR 12	LKR 15
LKR 13	LKR 20
LKR 14	LKR 10
LKR 15	LKR 27
LKR 16	LKR 5
LKR 17	LKR 24
LKR 18	LKR 17
LKR 19	LKR 13
LKR 20	LKR 21
LKR 21	LKR 21
LKR 22	LKR 21
LKR 23	LKR 7
LKR 24	LKR 0
LKR 25	LKR 2
LKR 26	LKR 2
LKR 27	LKR 2

8個の6ビット・セグメントと与えられる48個の置かれた番号キー・ビントは、各々6個の排他的オア回路(第3c、51及び38図にXORで示されている)より成る8個のモジュロ2加算器500、502、504、506、508、510、512及び514へ1入力として印加される。これと同時に、UDR200に与えられる32データ・ビントより取り出す8個の4ビット・セグメントと考えられるメッセージ・ブロックの第1半部分が、8個の6ビット・セグメントを形成する48個のデータ・ビントへ拡張されて、8個のモジュロ2加算器500~514の他の入力へ印加される。データ・ビントの拡張は、第3c、51及び38図に示されるように、8個の4ビット・セグメントの各々のエンド・ビント(図示の例では、各4ビット・セグメントの最初の2ビット)を二重にすることによって達成される。下記の表8及び表9に示されるように、8個のモジュロ2加算器500~514は、拡張された48個のデータ・ビント及び置かれた48個の番号キ

ー・ビントを組合わせて、8個の8ビットスライスアプライン制御機能ブロック500~504に対する各々の引数を形成する新しい8個の6ビット・セグメントを出力する。

表 8

ボウダスのマフティング計画

置かれた ビット番号	ビット番号	ボウダス・ビット番号	ボウダス番号
UDR 13	UDR 31	0	0
UDR 14	UDR	1	0
UDR 10	UDR 1	2	0
UDR 23	UDR 2	3	0
UDR 0	UDR 3	4	0
UDR 4	UDR 4	5	0
UDR 2	UDR 5	6	1
UDR 27	UDR 6	7	2
UDR 14	UDR 7	8	3
UDR 5	UDR 8	9	1
UDR 20	UDR 9	10	1
UDR 9	UDR 10	11	1
UDR 22	UDR 11	12	1
UDR 18	UDR 12	13	2
UDR 11	UDR 13	14	2
UDR 3	UDR 14	15	2
UDR 25	UDR 15	16	2
UDR 7	UDR 16	17	2
UDR 15	UDR 17	18	3
UDR 6	UDR 18	19	3
UDR 26	UDR 19	20	3
UDR 19	UDR 20	21	3
UDR 17	UDR 21	22	3
UDR 1	UDR 22	23	3

表 9

ボックスのマップビタリ数

置換された ビット番号	ビット番号	ボックス番号	ボックス番号
LBR 17	UDR 15	0	4
LBR 23	UDR 16	1	4
LBR 7	UDR 17	2	4
LBR 8	UDR 18	3	4
LBR 18	UDR 19	4	4
LBR 26	UDR 20	5	4
LBR 1	UDR 19	0	5
LBR 11	UDR 20	1	5
LBR 22	UDR 21	2	5
LBR 16	UDR 22	3	5
LBR 6	UDR 23	4	5
LBR 19	UDR 24	5	5
LBR 35	UDR 23	0	6
LBR 20	UDR 24	1	6
LBR 10	UDR 25	2	6
LBR 21	UDR 26	3	6
LBR 5	UDR 27	4	6
LBR 24	UDR 28	5	6
LBR 17	UDR 27	0	7
LBR 33	UDR 28	1	7
LBR 21	UDR 29	2	7
LBR 7	UDR 30	3	7
LBR 0	UDR 31	4	7
LBR 3	UDR 0	5	7

図3。図中の#08ボックス550の内部を第6図に示す。図示の如く、#08ボックス550はデコーダ552及びROM584から成っている。この#08ボックス550へは、#0モジュロ2加算器550からの6ビット・セグメントが入力として印加される。この6ビット・セグメントのエンド・ビット0及び5、即ち、二進化されたデータ・ビットUDR31及び置換された符号ヤ・ビットUKR13のモジュロ2加算と、二進化されたデータ・ビットUDR4及び置換された符号ヤ・ビットUKR4のモジュロ2加算とから生成されたビットを扱わず信号は、インバータ554及び556へ各々印加され、これによりエンド・ビットの補数信号が得られる。エンド・ビットのモジュロ2加算の結果が01であれば、各々16個のアンド回路を含む4グループの中の1つ、即ち、アンド回路568及び570を含む第1グループが選択される。同様に、エンド・ビットのモジュロ2加算の結果が01であれば、アンド回路572及び574を含む第2グループ

が選択され、結果が10であれば、アンド回路576及び578を含む第3グループが選択され、そして最後に結果が11であれば、アンド回路580及び582を含む第4グループが選択される。#08ボックス550へ印加される6ビット・セグメントの内側の4ビット(1, 2, 3, 4)を扱わず信号は、対応するインバータ558, 560, 562及び564へ各々印加され、これにより内側4ビットの補数信号が生成される。6ビット・セグメントの内側4ビットは、選択されたグループに含まれる16個のアンド回路の中の1つによつて解放され、ROM584の特定のアドレスへ出力信号を送る。ROM584は、基本的に4個の機能テーブル即ち0ROM, 1ROM, 2ROM及び3ROMで解放される。各機能テーブルは、16個のエントリを有しており、これらの各エントリは、素子586, 587, 588及び589の如き4個のPBT素子で実現され得る4ビットから成っている。これらの素子は、一旦選択されると、ROM584の出力線5

表 10

8 ボックス機能テーブル A

94, 595, 596 及び 597 へ一時的な4ピ
ント・セグメントを供給する。Cの4ピント・セ
グメントは、8 ボックス550の4本の出力線8
0, 91, 92 及び 93 の方へ送られる。

※30〜39に示される他の7個の8ボック
ス552, 554, 556, 558, 560, 5
62 及び 564 も、基本的に408 ボックス5
50と同様な構成であるが、各8ボックスに接
れる機能テーブルは互いに異なっており、従つて
8ボックスの異なる機能特性が与えられる。下記の
表10, 11, 12 及び 13 は、8個の8ボック
ス(※0〜※7)の機能テーブルの能力を示すも
ので、各出力を要する10進数は、英数字は4ピ
ントの2進パターン(例えば14 → 1110 など)
で出力される。

8 ボックスの 出力ピント	※08 ボックス				※18 ボックス			
	8 ボックスの エンド・ピント				8 ボックスの エンド・ピント			
	00	01	10	11	00	01	10	11
	(0)	(1)	(2)	(3)	(0)	(1)	(2)	(3)
0000 (0)	16	0	4	13	15	3	0	13
0001 (1)	4	15	1	13	1	13	14	8
0010 (2)	13	7	14	9	8	4	7	10
0011 (3)	1	4	9	2	14	7	11	1
0100 (4)	3	14	13	4	6	15	10	5
0101 (5)	15	2	6	9	11	2	4	15
0110 (6)	11	13	2	1	3	8	13	4
0111 (7)	8	3	11	7	4	14	1	2
1000 (8)	3	10	15	5	9	12	5	11
1001 (9)	10	6	12	11	7	0	8	6
1010 (10)	6	12	9	3	2	1	12	7
1011 (11)	12	11	7	14	13	10	6	12
1100 (12)	5	9	3	10	12	6	8	0
1101 (13)	9	5	10	0	0	9	3	9
1110 (14)	0	3	5	4	5	11	2	14
1111 (15)	7	8	0	11	10	5	15	9

表 11

8 ボックス機能テーブル B

8 ボックスの 出力ピント	※28 ボックス				※38 ボックス			
	8 ボックスの エンド・ピント				8 ボックスの エンド・ピント			
	00	01	10	11	00	01	10	11
	(0)	(1)	(2)	(3)	(0)	(1)	(2)	(3)
0000 (0)	10	13	15	1	7	13	10	9
0001 (1)	0	7	6	10	13	2	6	15
0010 (2)	9	0	4	13	14	11	5	0
0011 (3)	14	5	9	0	3	5	0	6
0100 (4)	6	3	8	6	0	6	12	19
0101 (5)	3	4	15	9	6	15	11	1
0110 (6)	15	4	3	8	9	0	7	13
0111 (7)	5	10	0	7	10	3	13	8
1000 (8)	1	2	11	4	1	4	15	9
1001 (9)	13	8	1	15	2	7	1	4
1010 (10)	12	5	2	14	8	2	3	5
1011 (11)	7	14	12	3	3	12	14	11
1100 (12)	11	12	5	11	11	7	5	12
1101 (13)	4	11	10	5	12	10	2	7
1110 (14)	2	15	14	2	4	14	8	2
1111 (15)	9	1	7	12	15	9	4	14

表 13

8 ボックス機能テーブル D

		#6 ボックス				#7 ボックス			
		8 ボックスの エンド・ビット				8 ボックスの エンド・ビット			
8 ボックスの FNC ビット		00	01	10	11	00	01	10	11
		(0)	(1)	(2)	(3)	(0)	(1)	(2)	(3)
0000 (0)		4	15	1	6	13	1	7	2
0001 (1)		11	0	4	11	7	15	3	1
0010 (2)		7	13	13	13	8	13	4	14
0011 (3)		14	7	13	8	4	8	1	7
0100 (4)		15	4	12	1	6	10	9	4
0101 (5)		0	9	3	4	15	3	12	10
0110 (6)		8	1	7	10	11	7	14	8
0111 (7)		12	10	14	7	1	4	2	13
1000 (8)		3	14	10	9	10	17	8	15
1001 (9)		12	3	15	5	9	5	6	12
1010 (10)		9	5	6	0	3	6	10	9
1011 (11)		1	12	8	11	24	11	13	0
1100 (12)		5	2	0	14	3	0	15	3
1101 (13)		10	15	5	2	0	14	3	5
1110 (14)		6	8	9	3	12	9	5	6
1111 (15)		1	6	2	12	7	2	9	11

表 12

8 ボックス機能テーブル C

		#4 ボックス				#5 ボックス			
		8 ボックスの エンド・ビット				8 ボックスの エンド・ビット			
8 ボックスの FNC ビット		00	01	10	11	00	01	10	11
		(0)	(1)	(2)	(3)	(0)	(1)	(2)	(3)
0000 (0)		2	14	4	11	12	10	9	4
0001 (1)		12	11	2	8	1	15	14	3
0010 (2)		8	2	1	12	10	4	15	2
0011 (3)		1	12	11	7	15	2	5	12
0100 (4)		7	4	10	1	9	7	2	9
0101 (5)		10	7	13	14	2	12	8	5
0110 (6)		11	13	7	2	6	9	12	15
0111 (7)		6	1	8	13	9	5	3	10
1000 (8)		8	5	15	6	0	6	7	11
1001 (9)		5	0	9	15	12	1	0	14
1010 (10)		3	15	12	0	3	11	4	1
1011 (11)		15	10	5	9	4	14	10	7
1100 (12)		13	3	6	10	14	0	1	6
1101 (13)		0	9	3	4	7	12	13	0
1110 (14)		14	8	0	5	5	3	11	8
1111 (15)		9	6	14	3	11	8	6	13

8個の8ボックス550～564は、32ビットの代替グループを規定する8個の4ビット・セグメントを供給し、次いでこれらのセグメントは、8ボックス00において、任意に決められた順序によつて變形変換される。8ボックス550～564で実行される非線形変換及び8ボックス00で実行される線形変換の結果、メッセージ・ブロックの第1半分の残ブロック番号が生成される。下記の表14は、8ボックスの出力の變形変換の様子を示したものである。

表 14

8ボックス出力の變形変換

8ボックス・ビット番号	生成されたビット番号
80	88
81	816
82	822
83	828
84	832
85	827
86	81
87	817
88	823
89	815
90	819
91	85
92	825
93	813
94	85
95	80
96	87
97	811
98	824
99	82
100	83
101	826
102	810
103	816
104	821
105	811
106	821
107	86
108	84
109	824
110	814
111	870
112	
113	
114	
115	
116	
117	
118	
119	
120	
121	
122	
123	
124	
125	
126	
127	
128	
129	
130	
131	
132	
133	
134	
135	
136	
137	
138	
139	
140	
141	
142	
143	
144	
145	
146	
147	
148	
149	
150	
151	
152	
153	
154	
155	
156	
157	
158	
159	
160	
161	
162	
163	
164	
165	
166	
167	
168	
169	
170	
171	
172	
173	
174	
175	
176	
177	
178	
179	
180	
181	
182	
183	
184	
185	
186	
187	
188	
189	
190	
191	
192	
193	
194	
195	
196	
197	
198	
199	
200	
201	
202	
203	
204	
205	
206	
207	
208	
209	
210	
211	
212	
213	
214	
215	
216	
217	
218	
219	
220	
221	
222	
223	
224	
225	
226	
227	
228	
229	
230	
231	
232	
233	
234	
235	
236	
237	
238	
239	
240	
241	
242	
243	
244	
245	
246	
247	
248	
249	
250	
251	
252	
253	
254	
255	
256	
257	
258	
259	
260	
261	
262	
263	
264	
265	
266	
267	
268	
269	
270	
271	
272	
273	
274	
275	
276	
277	
278	
279	
280	
281	
282	
283	
284	
285	
286	
287	
288	
289	
290	
291	
292	
293	
294	
295	
296	
297	
298	
299	
300	
301	
302	
303	
304	
305	
306	
307	
308	
309	
310	
311	
312	
313	
314	
315	
316	
317	
318	
319	
320	
321	
322	
323	
324	
325	
326	
327	
328	
329	
330	
331	
332	
333	
334	
335	
336	
337	
338	
339	
340	
341	
342	
343	
344	
345	
346	
347	
348	
349	
350	
351	
352	
353	
354	
355	
356	
357	
358	
359	
360	
361	
362	
363	
364	
365	
366	
367	
368	
369	
370	
371	
372	
373	
374	
375	
376	
377	
378	
379	
380	
381	
382	
383	
384	
385	
386	
387	
388	
389	
390	
391	
392	
393	
394	
395	
396	
397	
398	
399	
400	
401	
402	
403	
404	
405	
406	
407	
408	
409	
410	
411	
412	
413	
414	
415	
416	
417	
418	
419	
420	
421	
422	
423	
424	
425	
426	
427	
428	
429	
430	
431	
432	
433	
434	
435	
436	
437	
438	
439	
440	
441	
442	
443	
444	
445	
446	
447	
448	
449	
450	
451	
452	
453	
454	
455	
456	
457	
458	
459	
460	
461	
462	
463	
464	
465	
466	
467	
468	
469	
470	
471	
472	
473	
474	
475	
476	
477	
478	
479	
480	
481	
482	
483	
484	
485	
486	
487	
488	
489	
490	
491	
492	
493	
494	
495	
496	
497	
498	
499	
500	
501	
502	
503	
504	
505	
506	
507	
508	
509	
510	
511	
512	
513	
514	
515	
516	
517	
518	
519	
520	
521	
522	
523	
524	
525	
526	
527	
528	
529	
530	
531	
532	
533	
534	
535	
536	
537	
538	
539	
540	
541	
542	
543	
544	
545	
546	
547	
548	
549	
550	
551	
552	
553	
554	
555	
556	
557	
558	
559	
560	
561	
562	
563	
564	

第3a、51及び31図に示されるように、別の8個のモジュロ2加算器650、652、654、656、658、660、662及び664は、各々4個の排他的オア回路XORで構成される。LDR250に保持されているメッセージ・ブロックの第2半分(32データ・ビットより取り、8個の4ビット・データ・セグメントと考えられる)は、メッセージ・ブロックの第1半分の前ブロック暗号を挟む32ビットのグループと共に、これらのモジュロ2加算器650~664の入力へ印加される。モジュロ2加算器650~664は、これらの入力から、メッセージ・ブロックの更新された第2半分の新しい32ビットのグループを構成する8個の4ビット・セグメントを生成し、次いでこの新しい32ビットのグループは、母親を介して第3a図のUDR200へ転送される。

再び第3a図及び第7a図を参照するに、サイクル10の前半において、UDR200のすべてのランチャに接続されているLB線及びLDR線へ

信号が印加され、これによりメッセージ・ブロックの更新された第2半分を挟む32ビットのグループがUDR200へロードされる。これと同時に、LB線及びLDR線上の信号は、LDR250のすべてのランチャへも印加され、この結果、UDR200に記憶されていたメッセージ・ブロックの第1半分がLDR250のランチャへ転送されて、そこに記憶される。メッセージ・ブロックの第1半分及び更新された第2半分のこのような互換は、暗号化プロセスの次の繰返し操作を実行するための準備であり、これで、サイクル8における暗号キーの事前シフト後に開始された最初の繰返し操作が完了したことになる。

2回目の繰返し操作は、サイクル10、11及び12で実行され、サイクル10におけるシフト動作から開始される。最初のサイクル10の間に、8L線及びLDR線を介してUKR550及びLKR400のすべての座へ印加される第2信号により、暗号キーが更に1ビット位置だけシフト・アップされる。これは、暗号化プロセスの2回目

の繰返し操作に対する第2組の暗号キー・ビットを与えるものである。サイクル11においては、UDR200に記憶されているメッセージ・ブロックの更新された第2半分が、上述と同様な復ブロック暗号処理操作で使用され、次いでその結果がモジュロ2加算器650~664で処理されて、LDR250に記憶されているメッセージ・ブロックの第1半分が変更される。

サイクル12においては、UDR200のすべてのランチャに接続されているLB線及びLDR線への第2信号の印加により、メッセージ・ブロックの更新された第1半分の新しい32ビットのグループがUDR200に記憶される。これと同時に、LB線及びLDR線上の第2信号は、LDR250のすべてのランチャへも印加され、これによりUDR200に記憶されていたメッセージ・ブロックの更新された第2半分がLDR250へ転送されて、そこに記憶される。この互換操作は、暗号化プロセスの次の繰返しを実行するための準備であり、これで暗号化プロセスの2回目

の繰返し操作が完了される。

前記の第5の暗号キー・シフト計画に示されるように、暗号化プロセスの3回目の繰返し操作(サイクル11、12、13及び14で実行される)においては、暗号キーは2ビット位置だけシフトされなければならない。従って、サイクル11の間に8L線及びLDR線へ第3信号を印加することにより、暗号キーの2回のシフトのうちの最初のシフトが行なわれる。3回目の繰返し操作を実行するためのこの最初のシフト動作は、暗号装置内の分解時間の故に、8L線への第2信号の印加によつて開始された2回目の繰返し操作に対して影響を及ぼさない。暗号キーは、サイクル12の間に8L線及びLDR線へ印加される第4信号によつて、更に1ビット位置だけシフト・アップされる。このように、暗号キーは、3回目の繰返し操作の間に8L線及びLDR線へ印加される第3信号及び第4信号により、2ビット位置だけシフト・アップされる。

暗号化プロセスにおける最後の繰返し操作も、

同様にしてまた暗号キーのシフト計画に従って実行される。最後の決定し操作を除く残りの各繰返し操作においては、UKR350及びLKR400に記憶されている暗号キー・ビントは、所定のシフト計画に従ってシフトされ、LDR250に記憶されているメッセージ・ブロックの変更された半分は、UDR200に記憶されているメッセージ・ブロックの以前に変更された半分の横ブロック番号に従って再変更され、そしてモジュロ2加算値650~664からのこの再変更された半分は、メッセージ・ブロックの以前に変更された半分に代つてUDR200へロードされ、これと同時に、UDR200に記憶されていたこの以前に変更された半分は、LDR250へ転送されて、その前の内容に代つてそこに記憶される。

サイクル38及び39で実行される暗号化プロセスの最後の繰返し操作においては、UKR350及びLKR400に記憶されている暗号キー・ビントは、所定のシフト計画に従って最終シフトされ、そしてLDR250に記憶されているメッ

セージ・ブロックの変更された半分に対する最後の再変更が、UDR200に記憶されているメッセージ・ブロックの以前に変更された半分の横ブロック番号に従って実行される。しかしながら、サイクル39以降は、LB線上に信号が存在しないので、モジュロ2加算値650~664からの再変更された半分及びUDR200に記憶されている以前に変更された半分は互換されず、これらは元のメッセージ・ブロックの複暗号化ブロックを形成する。かくして、64ビットの複暗号化メッセージ・ブロックを要するUDR200からの32ビットの出力及びモジュロ2加算値650~664からの32ビットの出力は、対応するUOB700及びLOB750へ各々印加される。第3h、3i及び3j図に示されるように、UOB700は4個の8段シフト・レジスタUOB、1UOB、2UOB及び3UOBで構成され、同様に、LOB750も4個の8段シフト・レジスタULOB、1LOB、2LOB及び3LOBで構成される。図面には、最初のシフト・レジスタ

UOBの第1段(ランチャ702)、第2段(ランチャ704)及び最終段(ランチャ716)のみが詳細に示されているが、残りの段及び他のシフト・レジスタもこれと同じ構成である。

次に、第7b図をも参照して、これらのシフト・レジスタの動作について説明する。まずサイクル40において、UOB700及びLOB750の各シフト・レジスタのすべてのランチャに接続されているLDOD線及びLDOD線へ信号が印加され、これによりUDR200からUOB700への32ビット出力の並列転送及びモジュロ2加算値650~664からLOB750への32ビット出力の並列転送が同時に行なわれる。

UOB700及びLOB750へロードされた64ビットの複暗号化ブロックは、そこで一時に8ビット・バイトずつ並列-逐列変換を受け、各シフト・レジスタの最終段のビット内容が、1つの8ビット・バイトとしてPボックス800へ印加される。Pボックス800では、暗号化されたデータ・ビットをデータ・バス・アウトの適切な

ビット線へ接続するため、各8ビット・バイトに対する最後の順序変換が行なわれる。UOB700及びLOB750における並列-逐列変換は、8個の各シフト・レジスタUOB~3LOBの第2段から第8段までに、DO線及びLDO線を通じて信号を印加することによつて実行され、かくして、サイクル41~47の間に、各シフト・レジスタにあるデータ・ビットが1ビット位置ずつシフト・ダウンされる。各々の最終段からのビットで形成された8ビット・バイトは、上述のようにPボックス800で置換された後、データ・バス・アウトへ出力される。サイクル48において、64ビットの暗号化されたブロックの最後のバイトが転送され、これで暗号化プロセスが完了する。

第7a及び7b図には、次のメッセージ・ブロックを暗号化するためのサイクルは示されていないが、暗号化されるべきメッセージ・ブロックがあるとあつても、上と同じような方式で暗号化することが出来る。従つて、データの最初のメッ

セージ・ブロックが暗号化されている間に、もし次のメッセージ・ブロックが暗号装置に受取られると、このメッセージ・ブロックはUIB100及びLIB150にロードされる。サイクル59が終つて、最初の暗号化プロセスの繰返しの操作が完了すると、暗号キーはUKR350及びLKR400内で完全に1回転されて、元の状態に戻され、従つてアークの次のメッセージ・ブロックの暗号化を制御する準備ができています。最初の暗号化プロセスのサイクル40において、暗号化された最初のメッセージ・ブロックがUOB700及びLOB750へ転送されている間に、第7回図に破線で示されるように、LBT線及びLDR線へ信号を印加することにより、次のメッセージ・ブロックをUDR200及びLDR250へ転送することができ、そして次の暗号化プロセスは、最初のメッセージ・ブロックがUOB700及びLOB750からブロック800を介してデータ・バス・アウトへ転送されている間に、開始される。もし暗号装置に対するメッセージ・ブ

ロックの伝送率が高くなり過ぎて、前のメッセージ・ブロックが入力バッファからアーク・レジスタへ転送されてしまう前に次のメッセージ・ブロックが受信されるような状態が生じ得るならば、このような状態を知らせる(例えば、使用中信号を出す)ことのできる回路を設けなければならない。これは、後述のデータ・メッセージ・ブロックが暗号装置の動作速度において、同期的に伝送されるのを可能にする。

解読プロセス

本発明に従う暗号装置において、64ビットの暗号化されたデータ・メッセージ・ブロックを解読するための解読プロセスは、暗号化プロセスで用いられたのと同じ暗号キーの制御のもとに、同様の16回の繰返し操作を実行することによつて達成される。しかしながら、解読プロセスにおいては、暗号キーは、暗号化プロセスの場合のようには、最初の繰返し操作前に事前シフトされるのではなく、最後の繰返し操作後に事前シフトされる。

更に、暗号キーは、前記の図5に示されるシフト計画に従つて、暗号化プロセスの時とは反対の方向にシフトされる。これは、暗号化プロセスにおいて実行されたすべての繰返しを元に戻して、元のメッセージ・ブロックと同一の64ビットのメッセージ・ブロックを再生するように、解読繰返し操作時における暗号キー・ビットの適切な並列を確保に行なわせるものである。

図3a〜3d図及び第7回図を参照するに、前と同じようにサイクル0〜7において、暗号化されたデータ・メッセージ・ブロックはデータ・バス・インを介して受信された後、UIB100及びLIB150へバッファされ、そして暗号キーはUKR350及びLKR400へロードされる。続くサイクル8では、暗号化されたメッセージ・ブロックがUIB100からUDR200へ及びLIB150からLDR250へ各々並列に転送される。暗号化プロセスの時と同様に、サイクル9において、UDR200に記憶されている暗号化されたメッセージ・ブロックの第1半分が、

換された1組の暗号キー・ビットと共に複ブロック暗号処理操作で用いられ、その結果はモジュロ2加算時650〜664へ送られて、LDR250に記憶されているメッセージ・ブロックの第2半分を覆写するのに使用される。次のサイクル10では、LBT線へ印加される第1信号及びLDR線へ印加される信号により、暗号化されたメッセージ・ブロックの覆写された第2半分が、このメッセージ・ブロックの第1半分に代つてUDR200へ送られ、これと同時に、UDR200に記憶されていた第1半分は、暗号化されたメッセージ・ブロックの第2半分に代つてLDR250へ覆写される。これで、解読プロセスの次の繰返し操作に対する準備ができたことになる。

解読プロセスの2回目の繰返し操作は、サイクル10、11及び12で実行され、サイクル10の間に暗号キー・ビットを1ビット位置だけシフト・ダウンすることによつて開始される。暗号キー・ビットのシフト・ダウンは、8R線を介してUKR350及びLKRの第1線へ印加される

第1信号、S R線を介して残りの段へ印加される第1信号、正逆にL D K線を介してすべての段へ印加される信号の順回のもとに行なわれる。S R線上の第1信号は、L D K線上の信号と協働して、U K R 3 5 0及びL K R 4 0 0の各々の最終段のビット内容を各々の第1段へ転送させ、一万S R線上の第1信号は、L D K線上の信号と協働して、U K R 3 5 0及びL K R 4 0 0の各々のビット内容を各々の段へ転送させる。これにより、暗号キー全体の1ビット位置のシフト・ダウンが完了され、解読プロセスの2回目の繰返し操作のための新しい暗号キー・ビットの組が得られる。この2回目の繰返し操作は、暗号化プロセスのところで説明したのと同じようにして、サイクル12で完了される。

前記の段5に示されるように、解読プロセスの3回目の繰返し操作の開始時には、暗号キーは2ビット位置だけシフトされていなければならない。従つて、サイクル11の間に、S R線及びR K線へ第2信号を印加し且つL D K線へ信号を印加

することによつて、暗号キーの1回目のシフト動作が行なわれ、これにより暗号キーは1ビット位置だけシフト・ダウンされる。暗号キーの2回目のシフトは、サイクル12において、S R線及びR K線へ第3信号を印加し且つL D K線へ信号を印加することにより行なわれる。同様にして、また所定のシフト計画に従つて、解読プロセスの繰返しの繰返し操作が実行され、サイクル40で最初のプロセスが完了する。ただし、暗号化プロセスのところでも説明したように、16回目の繰返しにおいては、L B線へ信号が印加されないで、メッセージ・ブロックの第1半分及び第2半分の交換は行なわれない。次のメッセージ・ブロックの解読に対する準備のため、サイクル40の間に、暗号キーの最後のシフトが実行され、これにより暗号キーはU K R 3 5 0及びL K R 4 0 0内で完全に1回転されて、元の形に戻る。次いで、サイクル40~48の間に、解読されたデータ・メッセージ・ブロックは、U D R 2 0 0及びモジュロ2加算器650~664の出力からU O B 7 0

0及びL O B 7 5 0へ各々並列に転送された後、Pボックス800を介して一時に8ビット・バイトずつデータ・バス・アクトの方へ転送される。64ビットの構成されたデータ・メッセージ・ブロックの最後のバイトは、サイクル48で出力され、かくして解読プロセスが完了する。暗号化プロセスの時と同様、図7a及び7b図には示されていないが、繰返しの暗号化されたデータ・メッセージ・ブロックも同じようにして解読することができる。暗号化プロセスの間にモジュロ2加算器650~664で実行されたモジュロ2加算は、解読プロセスでのモジュロ2加算によつて逆転されるような自己逆転プロセス(self-reversing process)であることに注意されたい。

以上説明した本発明の実施例においては、一連のモジュロ2加算器500~514が使用されていたが、本ブロック暗号処理操作は、このようなモジュロ2加算器の使用だけに限定されるものではなく、48ビットの出力を与えるものであれば、任意の数の加算器又はこれらの加算器の組合わせ

を使用することができる。更に、本発明に従う暗号装置の構成は、データ・メッセージ・ブロック及び暗号キーのビット数に応じて、容易に変更されるものであり、上述の64ビットの例に限定されるものではない。また本発明に従う暗号装置は、暗号化及び解読の一方のみを実行するだけでなく、単に動作を逆にするだけで、両方のプロセスを同じ装置で実行し得るものである。

4. 図面の簡単な説明

第1図はデータ処理装置における暗号装置の概略場所を例示したブロック図。第2図は本発明に従う暗号装置の実施例を示したブロック図。第3図は第3a乃至3c図のつながりを明らかにしたブロック図。第3a乃至3c図は本発明に従う暗号装置の詳細なブロック図。第4図は本発明で使用するランダム数の具体例を示した図。第5図は第4図のランダム数の動作の様子を示したタイミング図。第6図は本発明で使用する8ビットの詳細を示した回路図。第7図は第7a及び7b図のつながりを明らかにしたブロック図。

第7a及び7b図は符号化及び解読プロセスのサイクルを示したタイミング図、第8図は符号化及び解読プロセスの繰返しの様子を示したブロック図である。

50 ... Pボックス、60 ... タイミング、100 ... 上部入力バッファ(UIB)、150 ... 下部入力バッファ(LIB)、200 ... 上部データレジスタ(UDR)、250 ... 下部データレジスタ(LDR)、300 ... Pボックス、350 ... 上部キーレジスタ(UKR)、400 ... 下部キーレジスタ(LKR)、450 ... Pボックス、500~514 ... モジュロ2加算器、550~564 ... 8ボックス、600 ... Pボックス、650~664 ... モジュロ2加算器、700 ... 上部出力バッファ(UOB)、750 ... 下部出力バッファ(LOB)、800 ... Pボックス。

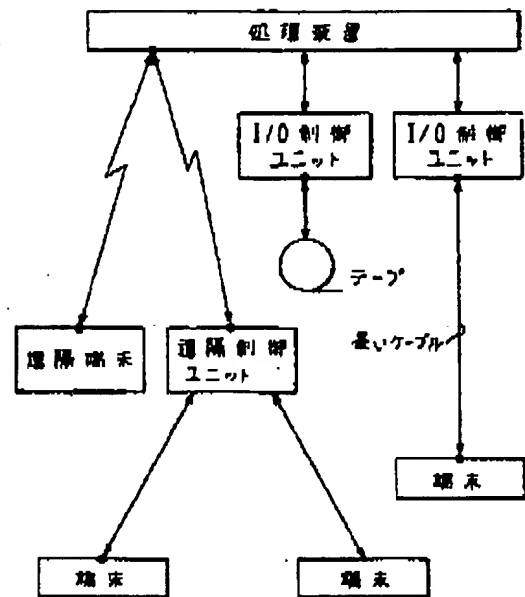


FIG. 1

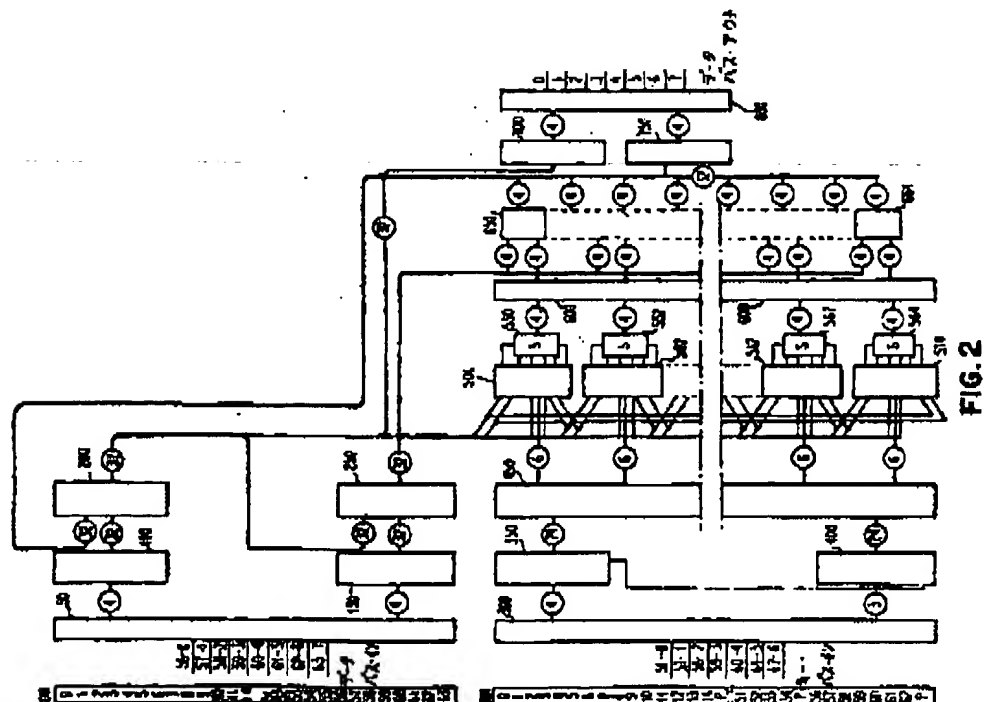
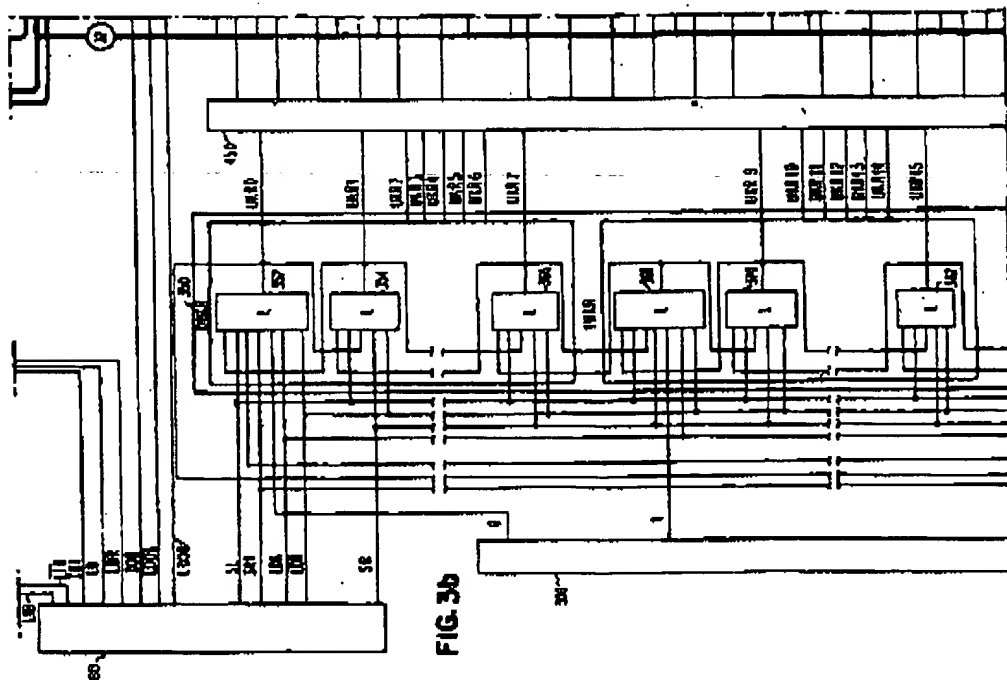
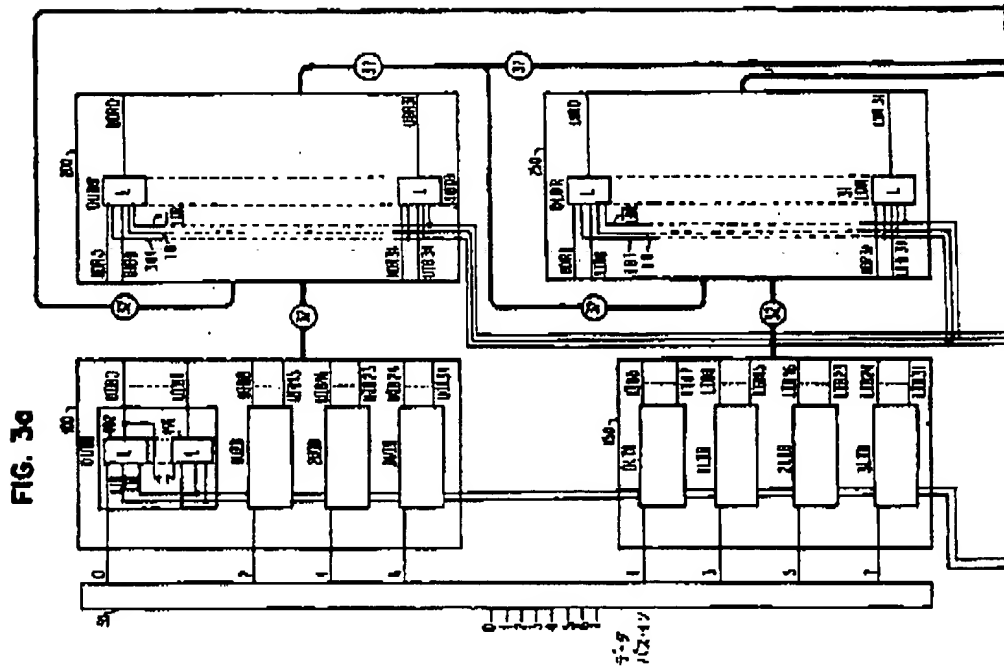
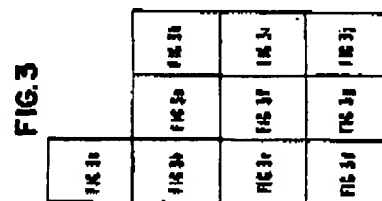
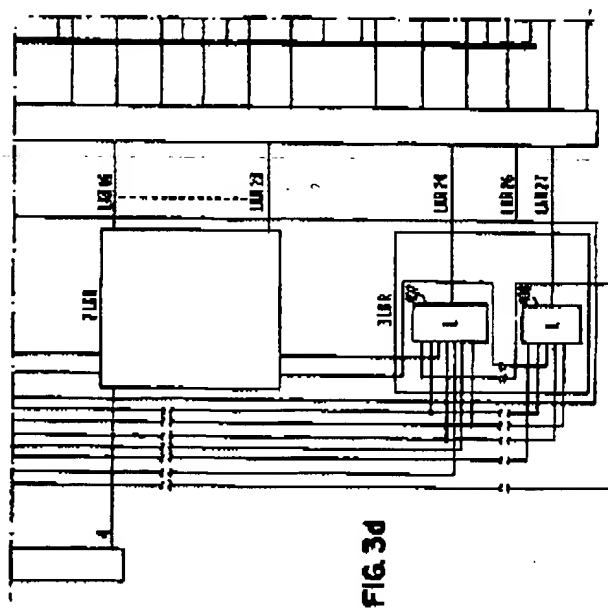
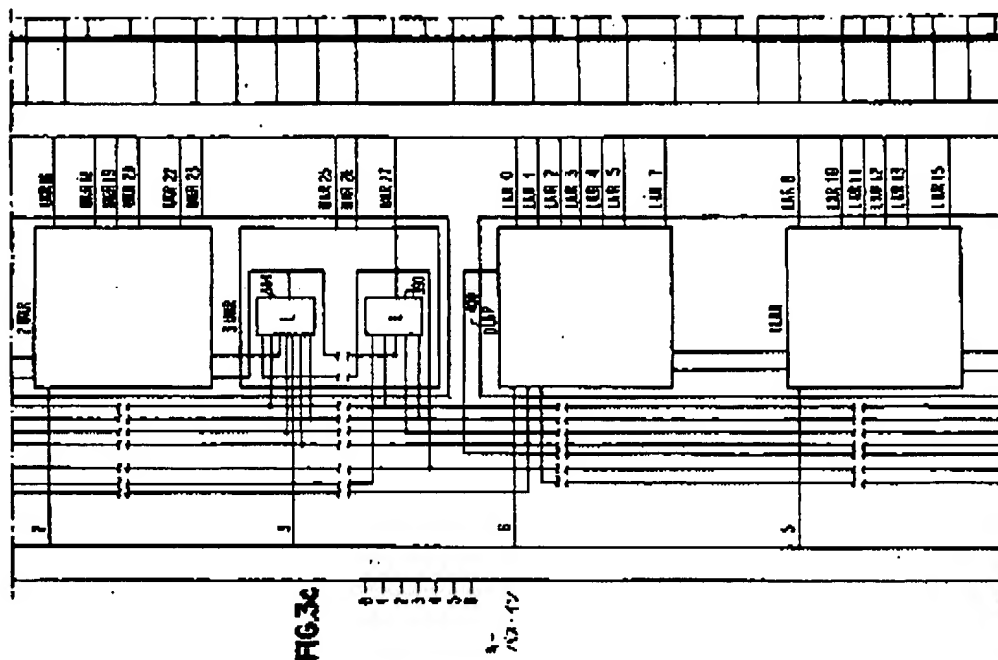
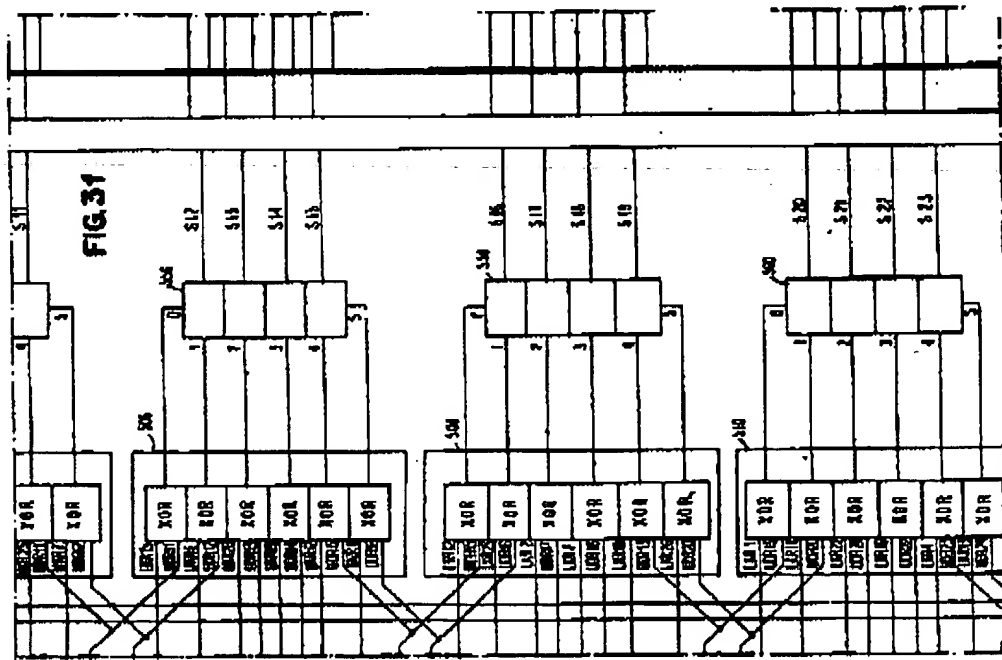
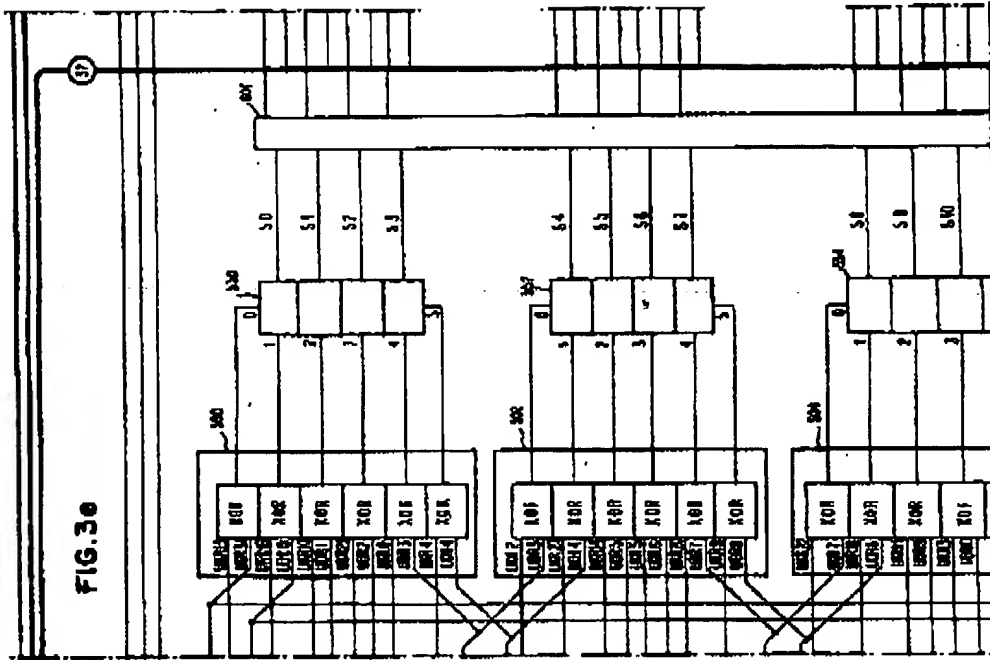


FIG. 2







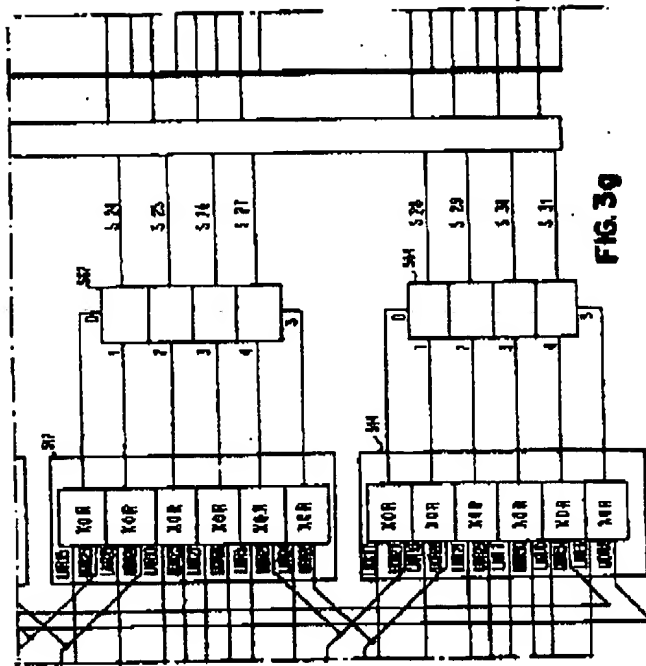


FIG. 5

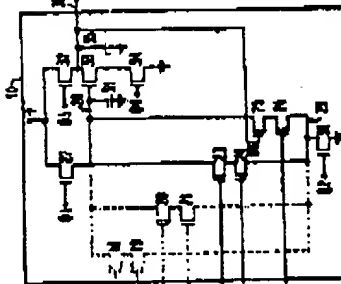
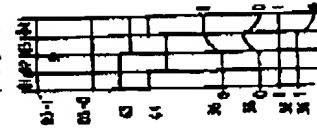
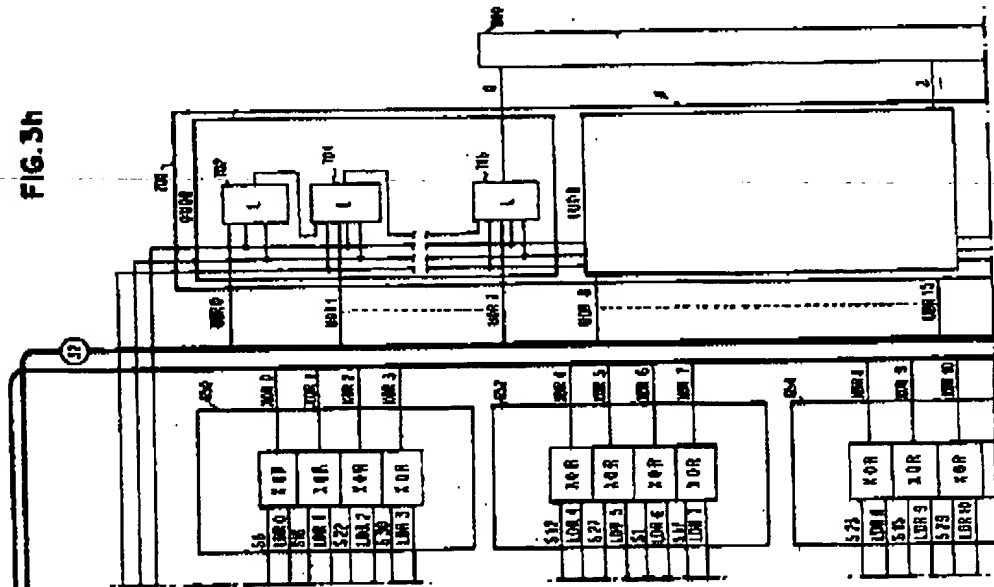


FIG. 4

FIG. 3h



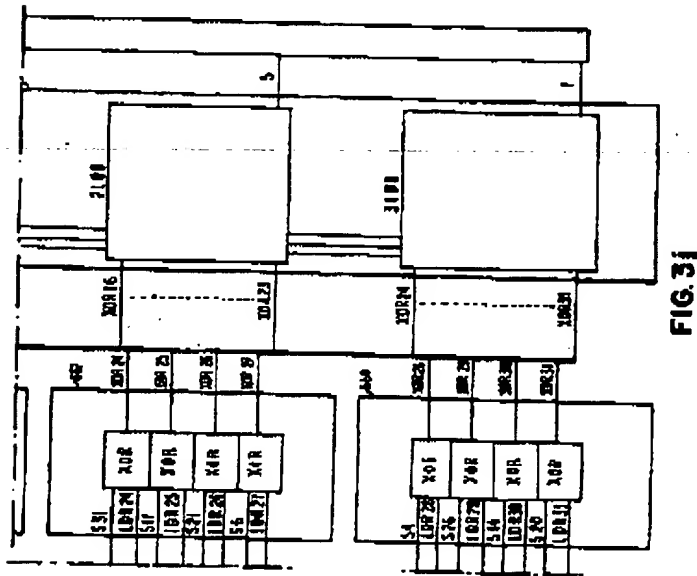
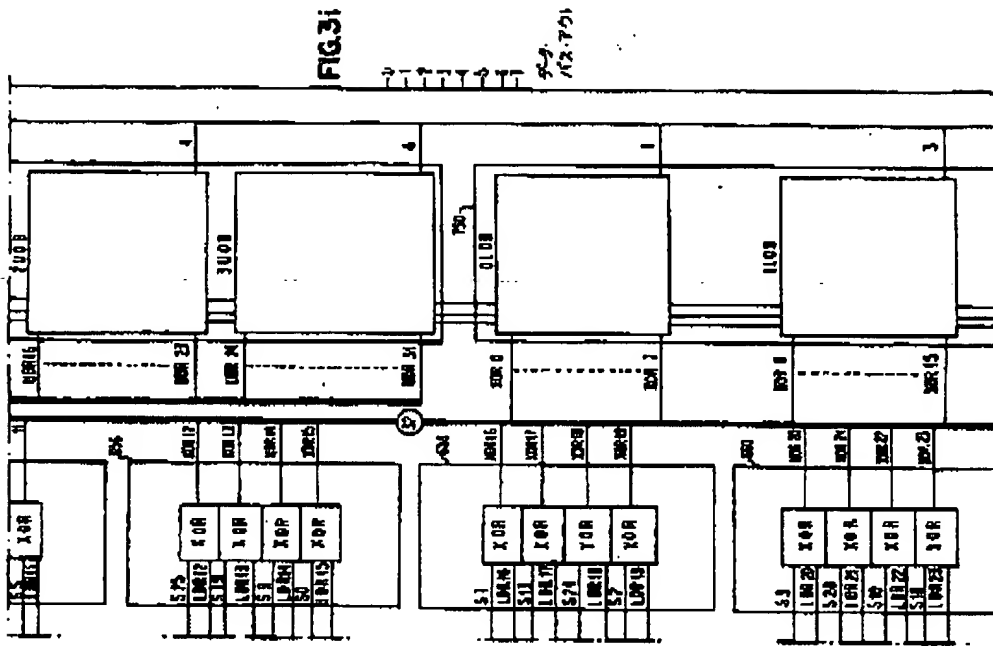


FIG. 7

FIG. 7a

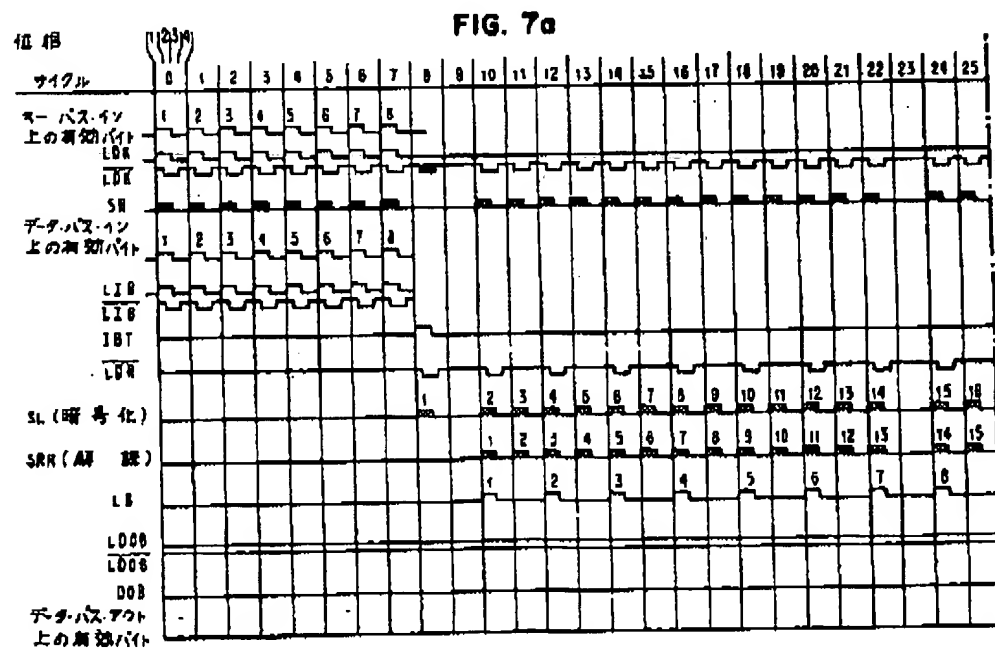
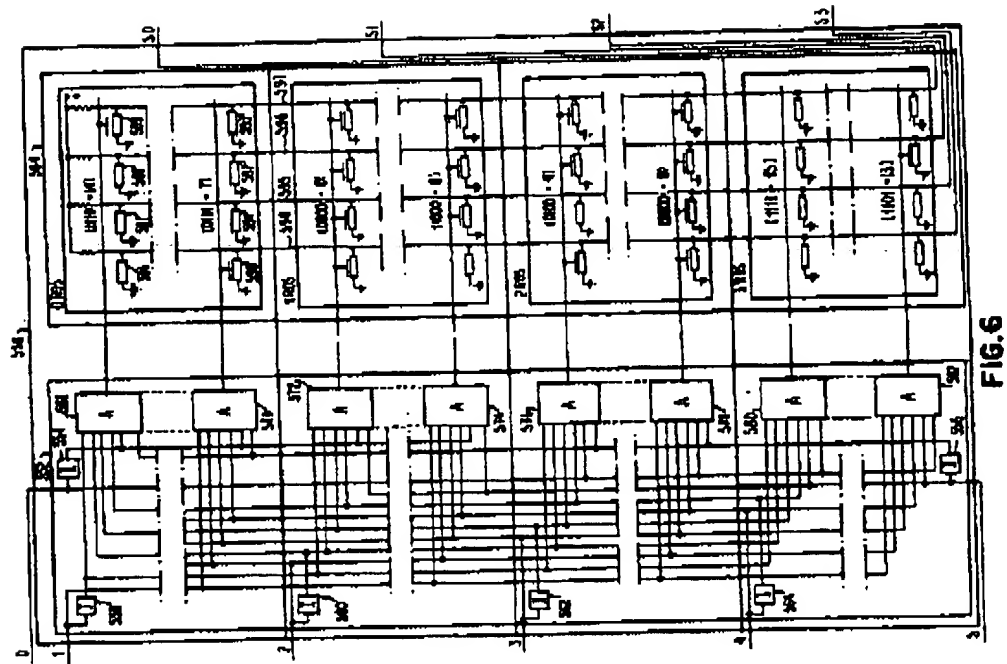


FIG. 7b

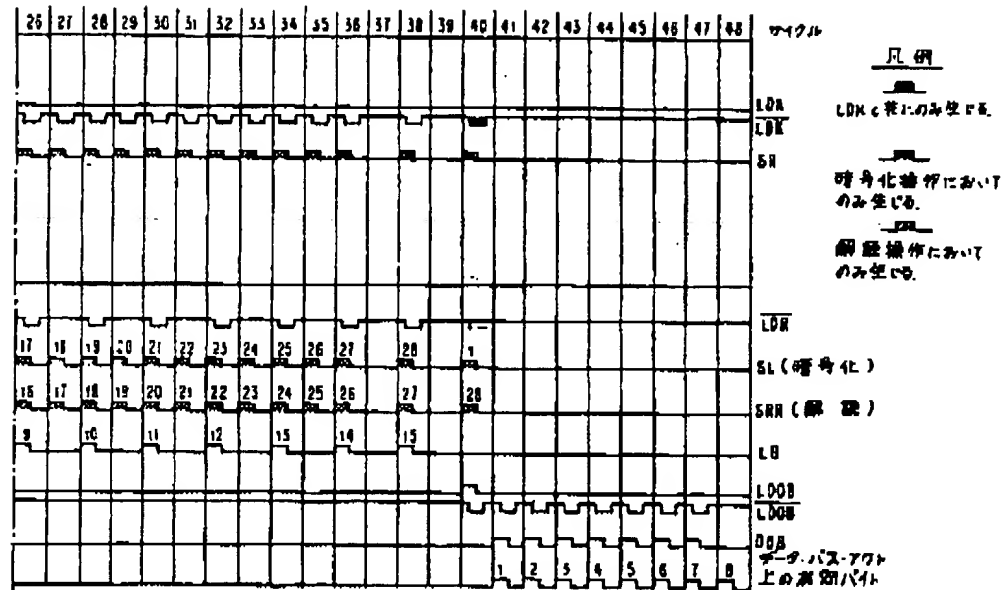
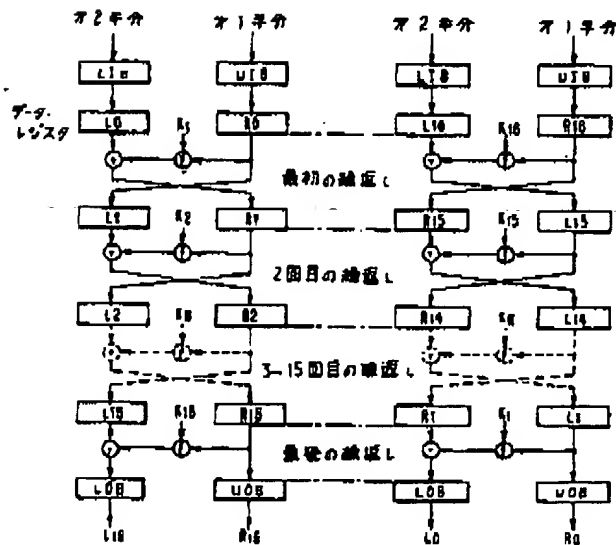


FIG. 8



暗号化

$$\begin{aligned}
 & \left\{ \begin{aligned} & L_{n+1} = R_n, \\ & L_n = L_{n-1} \oplus f(R_{n-1}, R_n), \\ & R_n = L_{n-1} \oplus f(R_{n-1}, R_n), \\ & R_n = R_{n-1}, \end{aligned} \right. \quad 1 \leq n \leq 16 \\
 & \left\{ \begin{aligned} & L_{n+1} = R_n \oplus f(L_n, R_n), \\ & L_{n+1} = L_n \oplus f(R_n, R_n), \\ & R_{n+1} = L_n, \\ & R_{n+1} = R_n, \end{aligned} \right. \quad 17 \leq n \leq 32
 \end{aligned}$$

解読

△ 前記以外の発明者又は代理人

(1) 発明者

任 所 アメリカ合衆国ニューヨーク州キンダストン、
ボクス223-11、アール グレー2、ルート28番地

氏 名 カール・エイ・ダブリュー・マイヤー

任 所 アメリカ合衆国ニューヨーク州ウェスト・ハーレー、
フィールドストーン・ロード12番地

氏 名 ロバート・エル・マワーズ

任 所 アメリカ合衆国ニューヨーク州ウインドストンク、
ホリー・ビル・ドライブ7番地

氏 名 ジョン・エル・スミス

任 所 アメリカ合衆国ニューヨーク州ウインドストンク、
ホワイトニー・ドライブ27番地

氏 名 ウォルター・エル・タフタマン

SUZUYE & SUZUYE

Jpn Pat. Appln. KOKAI Publication No. 51-108701

Filing No.: 51-16096

Filing Date: February 18, 1976

Applicant: International Business Machines Corporation

KOKAI Date: September 27, 1976

Request for Examination: Filed

Int.Cl.: H 04 K 1/00

H 04 L 9/00

G 06 F 3/00

Lines 7-16 of Upper Left Column of Page 3

The present invention provides an encrypting apparatus that can perform encrypting processing (encrypting or decrypting) with respect to a 32-bit data block under the control using one arbitrarily-selected encrypting key. The encrypting apparatus encrypts data by expanding a 32-bit data block into a 48-bit data block. The original data block includes eight segments each having four data bits, and the expanded data block includes eight segments each having six data bits.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.